MOBILE COMPUTING

ASST PROF. KAILAS I. PATIL

ME (CSE), BE (IT)

Information Technology

G H Raisoni Polytechnic, Jalgaon

PREFACE

This book is providing information for mobile computing .The most familiar aspect of mobile computing technology is the hand phone. About two decades ago, a hand phone was bulky and was only used for voice communication. It was merely an extension of the fixed line telephony that allowed users to keep in touch with colleagues. Now the hand phone is not only used for voice communication, it is also used to send text and multimedia messages. Future mobile devices will not only enable Internet access, but will also support high-speed data services.

In addition to the hand phone, various types of mobile devices are now available, for example, personal digital assistants (PDAs) and pocket personal computers (PCs). Road warriors use mobile devices to access up-to-date information from the corporate database. A police officer at a crime scene may send a fingerprint picked up there for matching with data in a central database through a wireless network, hence leading to faster identification and arrest of potential suspects. The global positioning system (GPS) is used in search and rescue missions, for monitoring and preservation of wildlife, and for vehicle theft prevention. Though many of us are unaware of when mobile computing technology is being used, it has permeated all aspects of our lives.

What is mobile computing? Simply defined, it is the use of a wireless network infrastructure to provide anytime, anywhere communications and access to information. There are many aspects of mobile computing and, sometimes, different terms are used to refer to them. This chapter gives an overview of what mobile computing has to offer and how it improves the quality of our lives. Later chapters discuss the underlying wireless networks and technologies that make mobile computing applications possible.

ACKNOWLEDGEMENT

I would like to express my gratitude to the many people who saw me through this book; to all those who provided support, talked things over, read, wrote, offered comments, allowed me to quote their remarks and assisted in the editing, proofreading and design. I would like to thank for enabling me to publish this book. Above all I want to thank my wife, Rama and the rest of my family, who supported and encouraged me in spite of all the time it took me away from them. It was a long and difficult journey for them. Perseverance, Inspiration & Motivation have always played a key role in the success of any venture.

At this level of understanding it is often difficult to understand the wide spectrum of knowledge without proper guidance and advice. Hence I take this opportunity to thanks for college staff to work under her valuable guidance, closely supervising this work, offering many innovative ideas and helpful suggestions, which led to the successful completion of this work. The college kept an eye on the progress of my work and always was available when I needed their advises.

I am especially thankful to my Aai, Papa & Wife and all other members of family who fully supported me during my work, who supported and encouraged me in spite of all the time it took me away from them.

I am also thankful to our Principal and Staff members for his warm support and providing all necessary facilities.

Kailas Ishwar Patil

TABLE OF CONTENTS

PREFACE i
ACKNOWLEDGEMENT ii
Chapter No. 1 Mobile Computing 1

1.1 Introduction to Mobile Computing……………………………………….………………………..1
1.2 Mobile Computing Devices……………………………………….…………………………..2
1.3 System Architecture……………………………………………………………………………4
1.4 Cellular System…………………………………………………………………………....6
    1.4.1The Cellular Concept………………………………….……………………………….6
        1.4.1.1 Frequency Reuse...8
        1.4.1.2 Channel Allocation Schemes…………………………….……………………..9
        1.4.1.3 Handoff Strategies…………………….……………………………………..9
        1.4.1.4 Interference and System Capacity…………….…………………….…………..10
1.5 Improving Coverage and Capacity………………………………………………………………13
    1.5.1 Cell Splitting……………………………………………………………………………13
    1.5.2 Sectoring…………………………………………………………………………………..15
    1.5.3 Microcell Zone Concept………………………………………………….…………15

Chapter No. 2 Global System for Mobile Communication (GSM)……………………...………………17

2.1 Introduction……………………………………………………………………………....17
2.2 GSM Services and Features…………………………………………………………………...17
2.3 What Is GSM?...18
2.4 Features of GSM………………………………………………………………………….....19
2.5GSM Architecture……………………………………………………………………………...20
2.6 GSM Network Areas……………………………………………..………………………23
2.7 Characteristics of the GSM Specification……………………………………………..…24
2.8 Mobile Subscriber ISDN Number………………………………………….………….…26
    2.8.1 Location Area Identity……………………………………………………………..…26
2.9 GSM User Services…………………………………………………………………….....27
2.10 GSM System Architecture……………………………………………………………………28
    2.10.1GSM Channel Types……………………………..……………………………………31
2.11 Frame Structure for GSM……………………...……………………………………….…40
2.12 Signal Processing in GSM……………………….……………………………………………43

Chapter No.03 GSM Mobility Management…………………………………………...…………..45

3.1 MOBILITY PROCEDURES IN GSM……………………………………………………………45
3.2 LOCATION UPDATING PROCEDURE……………………………………………. ……………45
    3.2.1 GSM location update……………………………………………..……………………..47
    3.2.2 Mobility Database………………………………………….…………………………......48

Chapter No. 4 General Radio Packet System (GPRS)…………………………………………………50

4.1 Introduction……………………………………………………………..…………….…50
4.2 Simple GPRS Technical Overview………………………………………….……………...52
    4.2.1SGSN……………………………………………………………………………………...53
    4.2.2GGSN……………………………………………………………………………………..54

4.2.3Connectivity between the SGSN & GGSN……………………………………………………54
4.2.4HLR…………………………………………………………………. …………..54
4.3 IP addressing……………………………………………………………………………………55
4.3.1Allocating Addresses……………………………………………………………………..55
4.4 GPRS Handset Classes…………………………………………………………………..………56
4.5 GPRS Architecture…………………………………………………………………………………..58
4.6 GPRS Mobile Stations, Base Station subsystem………………………………………………….……59
4.7 GPRS Network Nodes………………………………………………………………………………60
4.8 GPRS Network Operations………………………………………………………….………………61
4.9 Data Services in GPRS……………………………………………………………………………64

Chapter No-5 Mobile Security……………………………………………………………………….…78

5.1KEY FEATURES of Mobile Security……………………………………. ……………………………78
5.2 Threat Vectors Introduced by Mobile………………………………….……………………………….80
5.3 Countermeasures for data loss prevention on Mobile ………………………………………………82
5.4 Take Steps to Protect Your Mobile Phone……………………………………………….………..83
5.5 Act Quickly if Your Mobile Phone or PDA Is Stolen…………………………………….…………86
5.6 Implementation…………………………………………………………………………….…………87
5.7Attacks………………………………………………………………………………….…………..90
5.8 Component of Information Security………………………………………………………...….……93
5.9 Security Techniques and Algorithms …………………………………………………………….…95
5.10Smart Card Security ……………………………………………………………………….……..100

Chapter No. 6 Mobile Operating System…………………………………………………………….…..105

6.1 MOBILE OPERATING SYSTEMS……………………………………………………………...….105
6.2 MOBILE OPERATING SYSTEM POLICIES……………………………………………….……...109
6.3 Comparative Study of Different Mobile Operating Systems...114
6.4 TYPES OF MOBILE OS PLATFORMS...116
6.5 Mobile Operating System ……………………………………………..……………………117
6.6Android………………………………………………………………………….………………121
6.6.1Android Overview……………………………………………………………………………122
6.6.2Android Applications…………………………………………………………..…………...124
6.6.3Android Architecture……………………………………………………….…………….……125
6.6.4Life Cycle of Android Activity…………………………………………………………………..127

REFERENCES...129

Chapter No. 1

Mobile Computing

1.1 Introduction to Mobile Computing:

Mobile computing is an interaction between human and computer by which a computer is expected to be motivating during normal usage. Mobile computing involves software, hardware and mobile communication. Respectively, mobile software deals with the requirements of mobile applications. Also, hardware includes the components and devices which are needed for mobility. Communication issues include ad-hoc and infrastructure networks, protocols, communication properties, data encryption and concrete technologies.

Mobile computing means being able to use a computing device while changing location properties. Portability is one aspect of mobile computing .Also it is referred as the ability to use computing capability without a pre-defined location and/or connection to a network to for engaging data and information.

1.2 Mobile Computing Devices:

Many types of mobile computers have been introduced since the 1990s including the: personal digital assistant/enterprise digital assistant, smart phone, tablet computer, ultra-mobile PC, and wearable computer.

1. Personal Digital Assistant (PDA)

A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. PDAs are largely considered obsolete with the widespread adoption of smart phones.

Commonly current PDAs are able to connect to the Internet. A PDA has all requirements of connecting to internet such as: an electronic visual display, enabling it to include a web browser, audio capabilities enabling use as a portable media player. Most PDAs can access the Internet, intranets or extranets via wireless methods like Wi-Fi or Wireless Wide Area Networks. Most PDAs uses touch screen technology.

2. Smartphone

A Smartphone is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone.

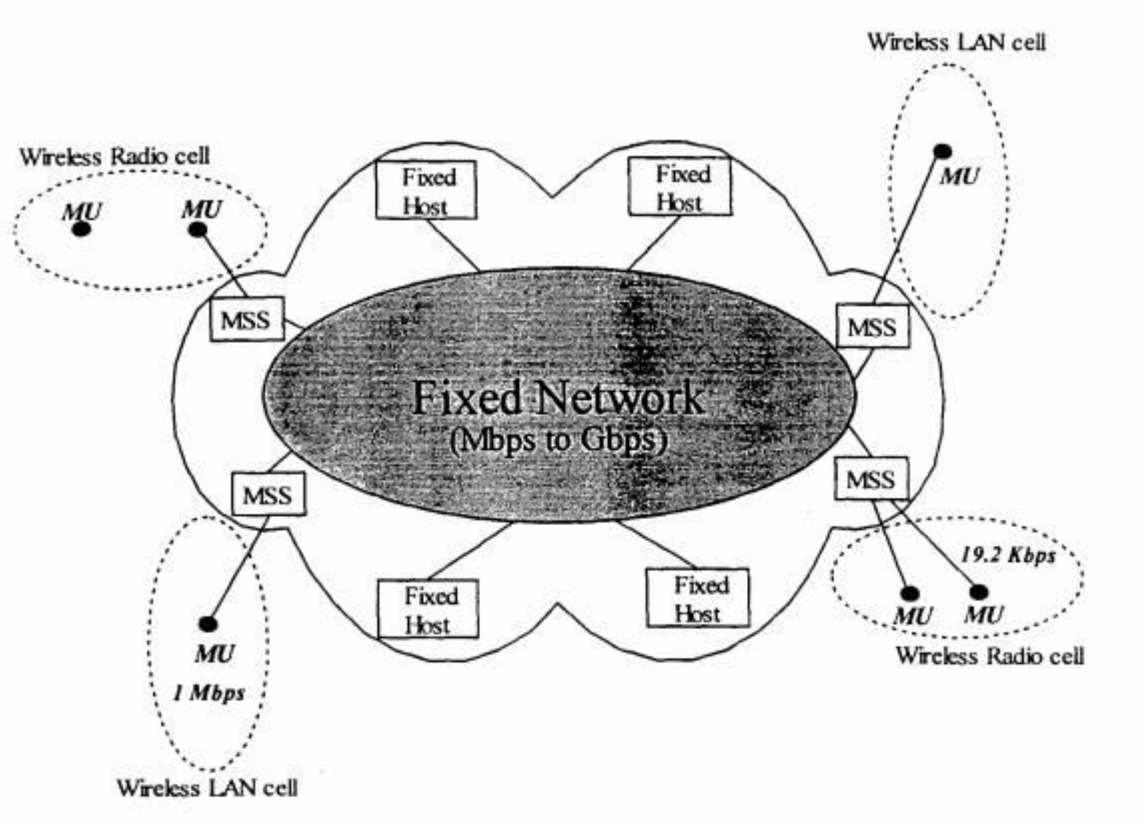
The first smart phones was a combination of a personal digital assistant (PDA) and a mobile phone functionally. Some functions were added in later models like portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units to form one multi-use device, high-resolution touch screens and web browsers for displaying standard web sites and mobile-optimized pages. Also, Wi-Fi provided high-speed data access and mobile broadband.

3. Tablet computer

Tablet computers are larger than a mobile phone or personal digital assistant. They are a type of mobile devices integrated into a flat touch screen and primarily operated by touching the screen. No physical keyboard is placed in them. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen. Normally, tablet does not have an integrated keyboard but they can be connected to a wireless or a USB keyboard, while notebook computers have an integrated keyboard that can be hidden by a slide joint. In hybrid models a detachable keyboard is included so that the touch screen can be used as a stand-alone tablet. Booklets include dual-touch screens. One of them is used as a virtual keyboard.

1.3 System Architecture:

A model view of the global architecture to support mobile wireless computing is show in Figure 1.1.The geographical area covered by a base station is called a 28 cell. Each cell is managed by a base station called the Mobile Support Station (MSS) (a fixed host) .



MU Mobile Unit (whether dumb terminal or walk stations),
MSS Mobile Support Station (equipped with wireless interface),
And Fixed Hosts (without wireless interface).

Fig. 1.1: Wireless Computing Architecture

The MSS is a server (transmitter) as well as the source of all data. The MSS can periodically broadcast data on the wireless network and the clients (units) can 'filter' the required data items. The MSS can also be the server in a client-server interaction (on-demand mode). In addition, the MSSs also provide commonly used application software, so that a mobile user can download the software from the closest MSS and run it on the palmtop. The wireless cells typically have restricted bandwidth. Due to constraints in the hardware, the wireless cells continue to have limited bandwidth. These cells may vary in terms of their wireless networks like satellite channel, radio channel, infra-red link etc. Wireless information services of the future are characterized by their geographical scope.

These services are classified as follows:

1. Pico services: Small Pico cells may have a very small range covering only relatively few clients. That is, these services will be very local and Pico cell will cover a few hundred meters in diameter. Examples of Pico services are as follows:

- Local parking availability of lot.
- Layout of the building.
- Empty seats in a stadium/restaurant
- Activities in Schools and colleges.
- Items in a store, and shopping mall advertising and local schemes

2. Micro services: The geographical area of Micro services (microcells) is provided in a range of few miles in diameter. Some of the Micro services include:

- Train and bus
- Station information.
- Local sports and cultural information.
- Local traffic information or airline information. o
- Local telephone directories information.

3. Macro services: These types of services could be provided in an area extended to tens of miles. These services are crucial on a regional basis (macrocells). Following are the examples of macro services:

- Regional maps.
- Weather information.
- Local news services are all instances of macro services.

4. **Wide Area Services:** The geographical area covered by these services is very large and these can be offered on a national basis. The examples of these services are as:

- Stock market information and national commodity prices.
- General political, financial and sports news are all examples of the wide area services.

1.4 Cellular System

1.4.1The Cellular Concept

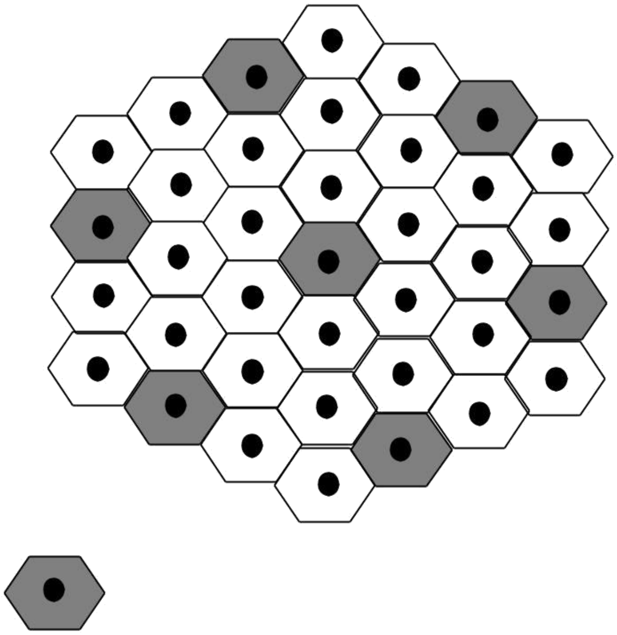
The design aim of early mobile wireless communication systems was to get a huge coverage area with a single, high-power transmitter and an antenna installed on a giant tower, transmitting a data on a single frequency. Although this method accomplished a good coverage, but it also means that it was practically not possible to reuse the same frequency all over the system, because any effort to reuse the same frequency would result in interference.

The mobile transceivers (also called mobile phones, handsets, mobile terminals or mobile stations) exchange radio signals with any number of base stations. Mobile phones are not linked to a specific base station, but can utilize any one of the base stations put up by the company. Multiple base stations covers the entire region in such a way that the user can move around and phone call can be carried on without interruption, possibly using more than one base station. The procedure of changing a base station at cell boundaries is called *handover*. Communication from the Mobile Station (MS) or mobile phones to the Base Station (BS) happens on an uplink channel also called reverse link, and downlink channel or forward link is used for communication from BS to MS. To maintain a bidirectional communication between a MS and BS, transmission resources must be offered in both the uplink and downlink directions. This can take place either using Frequency-Division Duplex (FDD), in which separate frequencies are used for both uplink and downlink channels, or through Time-Division Duplex (TDD), where uplink and downlink communications take place on the same frequency, but vary in time.

FDD is the most efficient technique if traffic is symmetric, and FDD has also made the task of radio planning more efficient and easier, because no interference takes place between base stations as they transmit and receive data on different frequencies. In case of an asymmetry in the uplink and downlink data speed, the TDD performs better than FDD. As the uplink data rate increases, extra bandwidth is dynamically allocated to that, and as the data rate decreases, the allotted bandwidth is taken away.

Some of the important cellular concepts are:

- Frequency reuse
- Channel Allocation
- Handoff
- Interference and system capacity
- Trunking and grade of service
- Improving coverage and capacity



Cells using the same set of Radio channels

Fig. 1.2: Cellular Network

1.4.1.1 Frequency Reuse

Conventional communication systems faced the problems of limited service area capability and ineffective radio spectrum utilization. This is because these systems are generally designed to provide service in an autonomous geographic region and by selecting radio channels from a particular frequency band. On the other hand, the present mobile communication systems are designed to offer a wide coverage area and high grade of service. These systems are also expected to provide a continuous communication through an efficient utilization of available radio spectrum. Therefore, the design of mobile radio network must satisfy the following objectives i.e., providing continuous service, and wide service area, while efficiently using the radio spectrum.

Fig. 1.2 shows the frequency reuse concept in a cell in a cellular network, in which cells utilize the same set of radio channels. The frequency reuse plan indicates where different radio channels are used. The hexagonal shape of cell is purely theoretical and is a simple model of radio coverage for each base station, although it has been globally adopted as the hexagon permits the easy analysis of a cellular system. The radio coverage of a cell can be calculated from field measurements. Although the actual radio coverage is very amorphous, a natural shape of a cell is required for an organized system design. While a circle is generally chosen to represent the coverage area of BS, but the circles present in the neighborhood cannot cover the entire region without leaving gaps or overlapping regions. Therefore, when selecting the cell shapes which can cover the entire geographical region without overlapping, there are three choices possible: a hexagon, square, and triangle. A particular design of the cell chosen in order to serve the weakest mobiles within the coverage area, and these are generally present at the cell boundaries of the cell. As hexagon covers the largest area from the center of a polygon to its farthest point, therefore, hexagon geometry can cover the entire geographic region to the fullest with minimum number of cells. When hexagon geometry is used to cover the entire geographic area, the base stations are either put up at the center of the cell, these cells are also called center excited cells or at the three of the six vertices (edge excited cells). Generally, center excited cells use omni-directional antennas and corner excited cells use directional antennas, but practically considerations for placing base stations are not exactly the same as they are shown in the hexagonal layouts.

1.4.1.2 Channel Allocation Schemes

For effective utilization of the radio spectrum, a channel reuse scheme is required which must be able to increase the capacity and reduce interference. Several channel allocation schemes have been proposed to address these objectives. Channel allocation schemes are classified into *fixed, dynamic, and hybrid.* The selection of a particular channel allocation scheme influences the performance of the system, mainly how to manage the calls when a call is handed-over from one cell to another.

In a fixed channel allocation scheme, a set of nominal channels are permanently allocated to each cell. Any call generated from within the cell can only be served by the idle radio channels present in that cell. If all the radio channels present in that cell are occupied, then the call is *blocked*. However, there exist a several variations of the fixed allocation. In one of the variation, a cell can borrow channels from neighboring cells if its own channels are already busy, and this scheme is called channel borrowing strategy. Such a borrowing procedure is being managed by mobile switching center (MSC) and it try to make sure that the borrowing of a radio channel form neighboring cells does not interfere with any of the existing calls present in the donor cell.

1.4.1.3 Handoff Strategies

When a mobile moves from one cell to another cell when a call is in progress, the MSC automatically shifts the call to a new channel present in the new cell. This handoff operation requires the identification of a new base station, and channels that are associated with the new base station.

In any cellular network, managing handoff is very important job. Many handoff schemes give high priority to handover requests over new call requests while allocating free channels, and it must be performed successfully and as infrequently as possible. Therefore, in order to satisfy these requirements, optimum signal at which to begin a handoff level must be specified by system designers.

Various systems have different methods for dealing with hand-off requests. Several systems manage handoff requests in the same way as they manage new call requests. In such systems, the possibility that a handoff call will not be served by a new base station is equivalent to the blocking probability of new calls. However, if a call is terminated unexpectedly while in progress is more frustrating than being blocked occasionally on a new call. Therefore, to improve the quality of service, various methods have been created to give priority to handoff call requests over new call requests while allocating channels.

1.4.1.4 Interference and System Capacity

Interference is one of the major factors affecting the performance of cellular radio systems. Sources of interference consist of another mobile inside the same cell, an ongoing call in a neighboring cell, other base stations transmitting signal in the same frequency band, or any non-cellular system which accidentally transmits energy into the cellular frequency band. Interference on voice signals could give rise to cross talk, where the caller hears interference in the background due to the presence of an unwanted transmission. The presence of interference in control channels, gives rise to missed and blocked calls. Interference is very dangerous in urban areas, due to the presence of larger base stations and mobile with greater RF noise. Interference has been accepted as a major obstruction in increasing the capacity of a system and is largely responsible for dropped calls in a network. The two major types of interferences that are taken consideration while allocating channels to the calls are *co-channel* and *adjacent channel interference*. While interfering signals are generated inside the cellular system by cellular transmitters, but they are difficult to control. The interference due to out-of-band users is very difficult to control, which happens without any word of warning, because of front end overload of subscriber equipment or intermittent inter-modulation products.

The co-channel interference can be reduced by the following methods:

a. *Increasing the distance (D) between two co-channel cells, D*

As D increases, the strength of interfering signal from co-channel interfering cells decreases significantly. But it is not wise to increase D because as D is increased, K must also be increased. High value of K means fewer number of radio channels are available per cell for a given spectrum. This results into decrease of the system capacity in terms of channels that are available per cell.

b. *Reducing the antenna heights*

Reducing antenna height is a good method to minimize the co-channel interference in some environment, e.g., on a high hill. In the cellular system design effective antenna height is considered rather than the actual antenna height. Therefore, the effective antenna height changes according to the present location of the mobile unit in such a difficult terrain.

When the antenna is put up on top of the hill, the effective antenna height gets more than the actual antenna height. So, in order to minimize the co-channel interference, antenna with lower height should be used without decreasing the received signal strength either at the cell-site or at the mobile device. Similarly, lower antenna height in a valley is very useful in minimizing the radiated power in a far-off high-elevation area where the mobile user is believed to be present.

However, reducing the antenna height does not always minimize the co-channel interference, e.g., in forests, the larger antenna height clears the tops of the longest trees in the surrounding area, particularly when they are located very close to the antenna. But reducing the antenna height would not be appropriate for minimizing co-channel interference because unnecessary attenuation of the signal would occur in the vicinity of the antenna as well as in the cell boundary if the height of the antenna is below the treetop level.

c. *Using directional antennas.*

The use of directional antennas in every cell can minimize the co-channel interference if the co-channel interference cannot be avoided by a fixed division of co-channel cells. This will also improve the system capacity even if the traffic increases. The co-channel interference can be further minimized by smartly setting up the directional antenna.

d. *Use of diversity schemes at the receiver.*

1.5 Improving Coverage and Capacity

As the demand for wireless service increases, the number of channels assigned to a cell eventually becomes to support the required number of users. At this point, cellular design techniques are needed to provide more channels per unit coverage area.Techniques such as cell splitting, sectoring, and coverage zone approaches are used in practice to expand the capacity of cellular systems. Cell splitting allows an orderly growth of the cellular system.

1.5.1 Cell Splitting

Cell splitting is a method in which congested (heavy traffic) cell is subdivided into smaller cells, and each smaller cell is having its own base station with reduction in antenna height and transmitter power. The original congested bigger cell is called macrocell and the smaller cells are called microcells. Capacity of cellular network can be increased by creating micro-cells within the original cells which are having smaller radius than macro-cells, therefore, the capacity of a system increases because more channels per unit area are now available in a network.

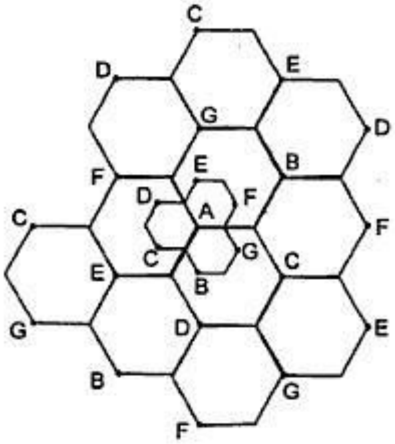


Fig. 1.3: Cell Splitting

Fig. 1.3 shows a cell splitting in which a congested cell, divided into smaller micro-cells, and the base stations are put up at corners of the cells. The micro-cells are to be added in such a way in order to the frequency reuse plan of the system should be preserved. For micro-cells, the transmit power of transmitter should be reduced, and each micro-cell is having half the radius to that of macro-cell.

In cell splitting, following factors should be carefully monitored;

1. In cell splitting, allocation of channels to the new cells (micro-cells) must be done very cautiously. So, in order to avoid co-channel interference, cells must follow the minimum reuse distance principle.

2. Power levels of the transmitters for new and old cells must be redesigned. If the transmitter of the old cell has the same power as that of new cells, then the channels in old cell interfere with the channels of new cell. But, if the power level of transmitter is too low then it may result into in sufficient area coverage.

3. In order to overcome the problem of point (2); the channels of macro-cell is divided into two parts. The channels in the first part are for the new cell and other part consists of channel for the old cell. Splitting of cells is done according to the number of subscribers present in the areas, and the power levels of the transmitters must be redesigned according to the allocated channels to old and new cells.

4. Antennas of different heights and power levels are used for smooth and easy handoff, and this technique is called Umbrella cell approach. Using this approach large coverage area is provided for high speed users and small coverage area to low speed users. Therefore, the number of call handoffs is maximized for high speed users and provides more channels for slow speed users.

5. The main idea behind cell splitting is the rescaling of entire system. In cell splitting, reuse factor (D/R) is kept constant because by decreasing the radius of cell (R) and, at the same time, the separation between co-channels (D) is also decreased. So, high capacity can be achieved without changing the (D/R) ratio of system.

1.5.2 Sectoring

Another way of improving the channel capacity of a cellular system is to decrease the D/R ratio while keeping the same cell radius. Improvement in the capacity can be accomplished by reducing the number of cells in a cluster, hence increasing the frequency reuse. To achieve this, the relative interference must be minimized without decreasing the transmit power.

1.5.3 Microcell Zone Concept

The micro-cell zone concept is associated with sharing the same radio equipment by different micro-cells. It results in decreasing of cluster size and, therefore, increase in system capacity. The micro-cell zone concept is used in practice to improve the capacity of cellular systems.

To improve both capacity and signal quality of a cellular system, cell sectoring depends upon correct setting up of directional antennas at the cell-site. But it also gives rise to increase in the number of handoffs and trunking inefficiencies. In a 3-sector or 6-sector

Cellular system, each sector acts like a new cell with a different shape and cell. Channels allocated to the un-sectored cell are divided between the different sectors present in a cell, thereby decreasing number of channels available in each sector. Furthermore, handoff takes place every time a mobile user moves from one sector to another sector of the same cell. This results in significant increase of network load on BSC and MSC of the cellular system. The problem of channel partitioning and increase in network load become very hard if all the 3 or 6-sectored directional antennas are placed at the centre of the cell.

In order to avoid delay, these zone-sites are connected through a high-speed fiber link to the base station. The base station first finds out, which of the three zone-sites has the better received signal strength from the mobile user and then that particular zone-site is used to transmit the signal to the mobile user. Therefore, only one zone-site is active at a time for communicating with the user and it also minimizes the co-channel interference experienced by the mobile user.

Advantages of micro zone concept:

1. When the mobile user moves from one zone to another within the same cell, the mobile user can keep the same channel for the call progress.
2. The effect of interference is very low due to the installation of low power transmitters.
3. Better signal quality is possible.
4. Fewer handoffs when a call is in progress.

Chapter No. 2

Global System for Mobile Communication (GSM)

2.1 Introduction

- Global System for Mobile (GSM) is a second generation cellular system standard that was developed to solve the fragmentation problems of the first cellular systems in Europe.

- GSM is the world's first cellular system to specify digital modulation and network level architectures and services. Before GSM, European countries used different cellular standards throughout the continent, and it was not possible for a customer to use a single subscriber unit throughout Europe.

2.2 GSM Services and Features

GSM services follow ISDN guidelines and are classified as either *teleservices* or *data services.* Teleservices include standard mobile telephony and mobile-originated or base-originated traffic. Data services include computer-to computer communication and packet-switched traffic. User services may be divided into three major categories:

1. Telephone services, including emergency calling and facsimile. GSM also supports Videotex and Teletex, though they are not integral parts of the GSM standard.

2. Bearer services or data services which are limited to layers 1, 2, and 3 of the open

system interconnection (OSI) reference model. Supported services include packet switched protocols and data rates from 300 bps to 9.6 kbps. Data may be transmitted using either a transparent mode (where GSM provides standard channel coding for the user data) or nontransparent mode (where GSM offers special coding efficiencies based on the particular data interface).

3. Supplementary ISDN services, are digital in nature, and include call diversion, closed user groups, and caller identification, and are not available in analog mobile networks. Supplementary services also include the *short messaging service*

2.3 What Is GSM?

- GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.

- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.

- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.

- GSM is the most widely accepted standard in telecommunications and it is implemented globally.

- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.

- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.

- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.

- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.

- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.

- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

2.4 Features of GSM

- Improved spectrum efficiency

- International roaming

- Low-cost mobile sets and base stations (BSs)

- High-quality speech

- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services

- Support for new services

2.5GSM Architecture

A GSM network comprises of many functional units. These functions and interfaces are explained in this chapter. The GSM network can be broadly divided into:

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

Given below is a simple pictorial view of the GSM architecture.

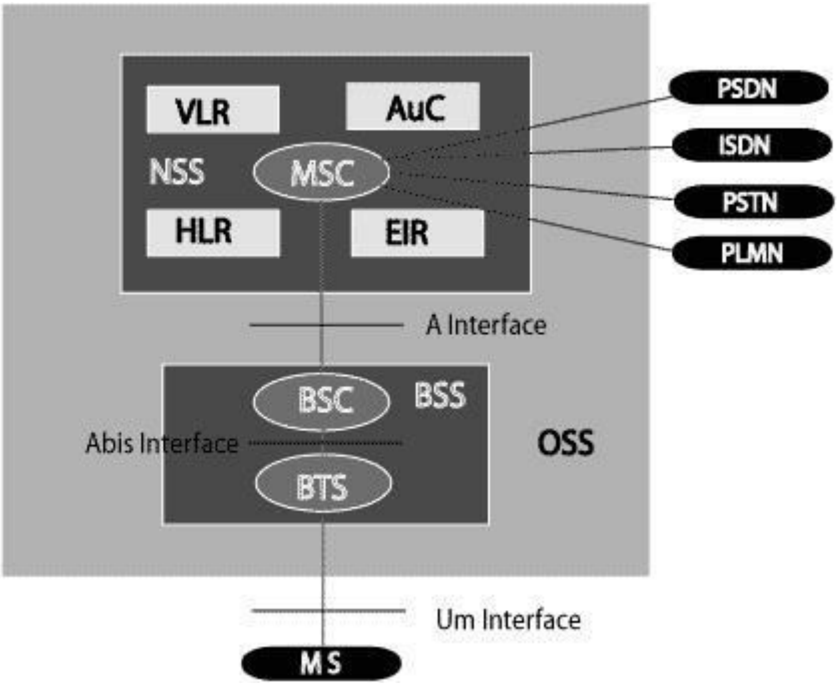


Fig. 2.1 GSM Architecture

The additional components of the GSM architecture comprise of databases and messaging systems’ functions:

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements:

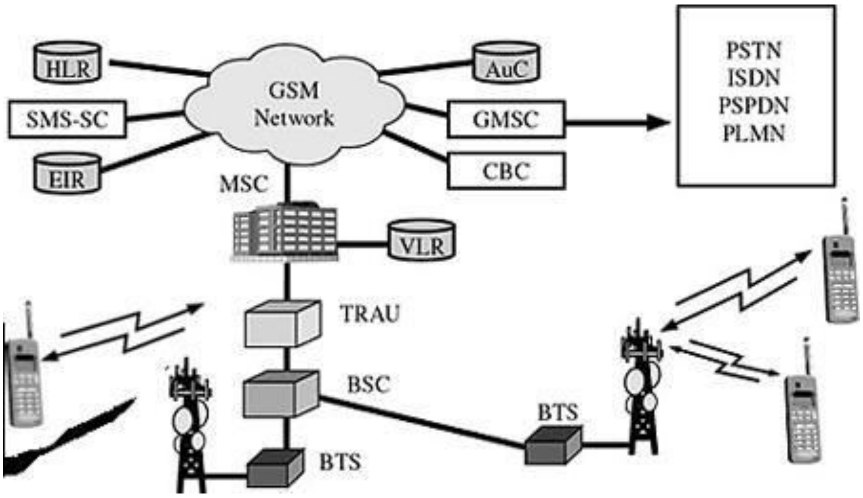


Fig. 2.2 GSM Network

The MS and the BSS communicate across the Um interface. It is also known as the *air interface* or the *radio link*. The BSS communicates with the Network Service Switching (NSS) center across the *A* interface.

2.6 GSM Network Areas

In a GSM network, the following areas are defined:

- **Cell:** Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

- **Location Area:** A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.

- **MSC/VLR Service Area:** The area covered by one MSC is called the MSC/VLR service area.

- **PLMN:** The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain one or more MSCs.

2.7 Characteristics of the GSM Specification

Modulation

Modulation is the process of transforming the input data into a suitable format for the transmission medium. The transmitted data is demodulated back to its original form at the receiving end. The GSM uses Gaussian Minimum Shift Keying (GMSK) modulation method.

Access Methods

Radio spectrum being a limited resource that is consumed and divided among all the users, GSM devised a combination of TDMA/FDMA as the method to divide the bandwith among the users. In this process, the FDMA part divides the frequency of the total 25 MHz bandwidth into 124 carrier frequencies of 200 kHz bandwidth.

Each BS is assigned with one or multiple frequencies, and each of this frequency is divided into eight timeslots using a TDMA scheme. Each of these slots are used for both transmission as well as reception of data. These slots are separated by time so that a mobile unit doesn’t transmit and receive data at the same time.

Transmission Rate

The total symbol rate for GSM at 1 bit per symbol in GMSK produces 270.833 K symbols/second. The gross transmission rate of a timeslot is 22.8 Kbps.

GSM is a digital system with an over-the-air bit rate of 270 kbps.

Frequency Band

The **uplink frequency range** specified for GSM is 933–960 MHz (basic 900 MHz band only). The **downlink frequency band** is 890–915 MHz (basic 900 MHz band only).

Channel Spacing

Channel spacing indicates the spacing between adjacent carrier frequencies. For GSM, it is 200 kHz.

Speech Coding

For speech coding or processing, GSM uses Linear Predictive Coding (LPC). This tool compresses the bit rate and gives an estimate of the speech parameters. When the audio signal passes through a filter, it mimics the vocal tract. Here, the speech is encoded at 13 kbps.

Duplex Distance

Duplex distance is the space between the uplink and downlink frequencies. The duplex distance for GSM is 80 MHz, where each channel has two frequencies that are 80 MHz apart.

2.8 Mobile Subscriber ISDN Number:-

The authentic telephone number of a mobile station is the Mobile Subscriber ISDN Number (MSISDN). Based on the SIM, a mobile station can have many MSISDNs, as each subscriber is assigned with a separate MSISDN to their SIM respectively.

Listed below is the structure followed by MSISDN categories, as they are defined based on international ISDN number plan:

- **Country Code (CC) :** Up to 3 decimal places.
- **National Destination Code (NDC):** Typically 2–3 decimal places.
- **Subscriber Number (SN):** Maximum 10 decimal places.

2.8.1 Location Area Identity

Within a PLMN, a Location Area identifies its own authentic Location Area Identity (LAI). The LAI hierarchy is based on international standard and structured in a unique format as mentioned below:

- **Country Code (CC):** 3 decimal places.
- **Mobile Network Code (MNC):** 2 decimal places.
- **Location Area Code (LAC):** maximum 5 decimal places or maximum twice 8 bits coded in hexadecimal (LAC < FFFF).

2.9 GSM User Services

GSM offers much more than just voice telephony. Contact your local GSM network operator to the specific services that you can avail.

GSM offers three basic types of services:

- Telephony services or teleservices
- Data services or bearer services
- Supplementary services

Teleservices

The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

Voice Calls

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

Videotext and Facsimile

Another group of teleservices includes Videotext access, Teletex transmission, Facsimile alternate speech and Facsimile Group 3, Automatic facsimile Group 3, etc.

Shot Text Messages

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

2.9 GSM System Architecture

- The GSM system architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces.

- The subsystems are the *Base Station Subsystem* (BSS), *Network and Switching Subsystem* (NSS), and the *Operation Support Subsystem* (088).

- The *Mobile Station* (MS) is also a subsystem, but is usually considered to be part of the BSS for architecture purposes. Equipment and services are designed within GSM *to* support *one or* more of these specific subsystems.

- The BSS, also known as the *radio subsystem,* provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). The BSS also manages the radio interface between the mobile stations and all other subsystems of GSM. Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the NSS via the MSCs.

- The NSS manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN. Figure shows the block diagram of the GSM system architecture.

- The Mobile Stations (MS) communicate with the Base Station Subsystem (BSS) over the radio air interface. The BSS consists of many BSCs which connect to a single

MSC, and each BSC typically controls up to several hundred *Base 1Tansceiver Stations* (BTSs).

- Some of the BTSs may be co-located at the BSC, and others may be remotely distributed and physically connected to the BSC by microwave link or dedicated leased lines. Mobile handoffs (called *handovers,* or HO, in the GSM specification) between two BTSs under the control of the same BSC are handled by the BSC, and not the MSC. This greatly reduces the switching burden of the MSC.

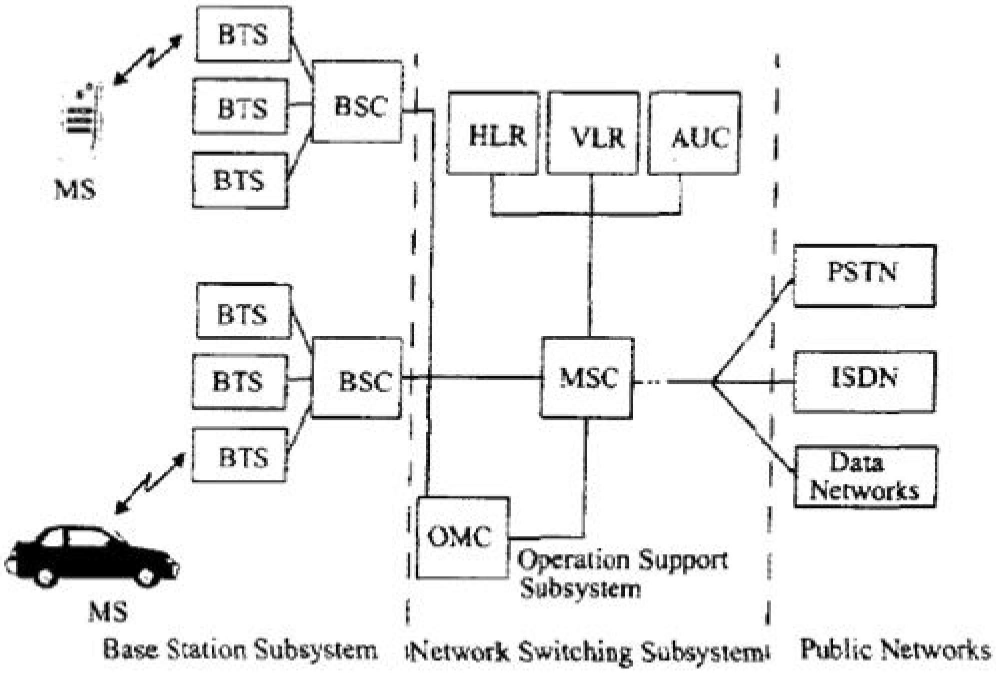


Fig. 2.3 GSM System Architecture

- As shown in Figure, the interface which connects a BTS to a BSC is called the A_{bis} *interface.*

- The A_{bis} interface carries traffic and maintenance data, and is specified by GSM to be standardized for all manufacturers.

- In practice, however, the A_{bis} for each GSM base station manufacturer has subtle differences, thereby forcing service providers to use the same manufacturer for the BTS and BSC equipment.

- The BSCs are physically connected via dedicated/leased lines or microwave link to the MSC. The interface between a BSC and a MSC is called the *A interface,* which is standardized within GSM.

- The *A* interface uses an SS7 protocol called the *Signaling Correction Control Part* (SCCP) which supports communication between the MSC and the BSS, as well as network messages between the individual subscribers and the MSC.

- The *A* interface allows a service provider to use base stations and switching equipment made by different manufacturers.

2.10.1GSM Channel Types

- There are two types of GSM logical channels, called *traffic channels* (TCH) and *control channels* (CCH) .

- Traffic channels carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link.

- Control channels carry signaling and synchronizing commands between the base station and the mobile station.

- Certain types of control channels are defined for just the forward or reverse link. There are six different types of TCHs provided for in GSM, and an even larger number of CCHs, both of which are now described.

1. GSM Traffic Channels (TCH)

- GSM traffic channels may be either full-rate or half-rate and may carry either digitized speech or user data.

- When transmitted as full-rate, user data is contained within one TS per frame. When transmitted as half-rate, user data is mapped onto the same time slot, but is sent in alternate frames.

- That is, two half-rate channel users would share the same time slot, but would alternately transmit during *every* other frame. In the GSM standard, TCH data may not be sent in TS 0 within a TDMA frame on certain ARFCNs which serve as the broadcast station for each cell (since this time slot is reserved for control channel bursts in most every frame, as described subsequently).

- Furthermore, frames of TCH data are broken up every thirteenth frame by either slow associated control channel data (SACCH) or idle frames. Illustrates how the TCH data is transmitted in consecutive frames.

- Each group of twenty-six consecutive TDMA frames is called a *multiframe* (or *speech multiframe,* to distinguish it from the control channel multiframe described below).

- For *every* twenty-six frames, the thirteenth and twenty-sixth frames consist of Slow Associated Control Channel (SACCH) data, or the idle frame, respectively. The twenty-sixth frame contains idle bits for the case when full-rate TCHs are used, and contains SACCH data when half-rate TCHs are used.

A. Full-Rate TCH

The following full rate speech and data channels are supported:

• **Full-Rate Speech Channel (TCH/FS)** -The full-rate speech channel carries user speech which is digitized at a raw data rate of 13 kbps. With GSM channel coding added to the digital speech, the full-rate speech channel carries 22.8 kbps.

- **Full-Rate Data Channel for 9600 bps (TCHIF9.6)** - The full-rate traffic data channel carries raw user data which is sent at 9600 bps. With additional forward error correction coding applied by the GSM standard, the9600 bps data is sent at 22.8 kbps.

- **Full-Rate Data Channel for 4800 bps (TCHIF4.8)-**The full-rate traffic data channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by the GSM standard, the4800 bps is sent at 22.8 kbps.

- **Full-Rate Data Channel for 2400 bps (TCH/F2.4)-**The full-rate traffic data channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by the GSM standard, the2400 bps is sent at 22.8 kbps.

B. Half-Rate TCH

The following half-rate speech and data channels are supported:

- **Half-Rate Speech Channel (TCH/HS)** - The half-rate speech channel has been designed to carry digitized speech which is sampled at a rate half that of the full-rate channel GSM anticipates the availability of speech coders which can digitize speech at about 6.5 kbps. With GSM channel coding added to the digitized speech, the half-rate speech channel will carry 11.4 Kbps.

- **Half-Rate Data Channel for 4800 bps (TCH/114.8)-**The half-rate traffic data channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by the GSM standard, the4800 bps data is sent at 11.4 kbps.

- **Half-Rate Qata Channel for 2400 bps (TCH/112.4)-**The half-rate traffic data channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by the GSM standard, the2400 bps data is sent at 11.4 kbps.

‘

2. GSM Control Channels (CCH)

- There are three main control channels in the GSM system. These are the *broadcast channel* (BCH), the *common control channel* (CCCH), and the *dedicated control channel* (DCCH).

- Each control channel consists of several logical channels which are distributed in time to provide the necessary GSM control functions.

- The GSM specification defines thirty-four ARFCNs as standard broadcast channels. For each broadcast channel, frame 51 does not contain any BCHI CCCH forward channel data and is considered to be an idle frame.

- However, the reverse channel CCCH is able to receive subscriber transmissions during TS 0 of any frame (even the idle frame). On the other hand, DCCH data may be sent during any time slot and any frame, and entire frames are specifically dedicated to certain DCCH transmissions. GSM control channels are now described in detail.

3. Broadcast Channels (BCH):

The broadcast channel operates on the forward link of a specific ARFCN within each cell, and transmits data only in the first time slot (TS 0) of certain GSM frames. Unlike TCHs which are duplex, BCHs only use the forward link.

The three types of BCH are now described.

(a) ***Broadcast Control Channel (BCCH)***-The BCCH is a forward control channel that is used to broadcast information such as cell and network identity, and operating characteristics of the cell (current control channel structure, channel availability, and congestion). The BCCH also broadcasts a list of channels that are currently in use within the cell.

(b) ***Frequency Correction Channel (FCC H)***- The FCCH is a special data burst which occupies TS 0 for the very first GSM frame (frame 0) and is repeated every ten frames within a control channel multiform. The FCCH allows each subscriber unit to synchronize its internal frequency standard (local oscillator) to the exact frequency of the base station.

(c) ***Synchronization Channel (SCH)*-**SCH is broadcast in TS 0 of the frame immediately following the FCCH frame and is used to identify the serving base station while allowing each mobile to frame synchronize with the base station. The *frame number* (FN), which ranges from 0 to 2,715,647, is sent with the *base station identity code* (BSIC) during the SCH burst. The BSIC is uniquely assigned to each BST in a GSM system.

These channels are described below.

(a) ***Paging Channel (PCH)*** - The PCH provides paging signals from the base station to all mobiles in the cell, and notifies a specific mobile of an incoming call which originates from the PSTN. The PCH transmits the IMSI of the target subscriber, along with a request for acknowledgment from the mobile unit on the RACH. Alternatively, the PCH may be used to provide *cell broadcast* ASCII text messages to all subscribers, as part of the SMS feature of GSM.

(b) ***Random Access Channel (RACH)-***The Rachis a reverse link channel used by a subscriber unit to acknowledge a page from the PCH, and is also used by mobiles to originate

a call. The RACH uses a slotted ALOHA access scheme. All mobiles must request access or respond to a PCH alert within TS 0 of a GSM frame. At the BTS, every frame (even the idle frame) will accept RACH transmissions from mobiles during TS 0

(c) Access ***Grant Channel (AGCH)***- 'the AGCH is used by the base station to provide forward link communication to the mobile, and carries data which instructs the mobile to operate in a particular physical channel (time slot and ARFCN) with a particular dedicated control channel The AGCH is the final CCCH message sent by the base station before a subscriber is moved off the control channel The AGCH is used by the base station to respond to a BACH sent by a mobile station in a previous CCCH frame.

4. Dedicated Control Channels (DCCH):

There are three types of dedicated control channels in GSM, and, like traffic channels, they are bidirectional and have the same format and function on both the forward and reverse links. Like TCHs, DCCHs may exist in any time slot and on any ARFCN *except TSO* of the BCH ARFCN.

(a) ***Stand-alone Dedicated Control Channels (SDCCH)***- The SDCCH carries signaling data following the connection of the mobile with the base station, and just before a TCH assignment is issued by the base station. The SDCCH ensures that the mobile station and the base station remain connected while the base station and MSC verify the subscriber unit and allocate resources for the mobile. The SDCCH can be thought of as an intermediate and temporary channel which accepts a newly completed call from the BCH and holds the traffic while waiting for the base station to allocate a TCH channel.

(b) ***Slow Associated Control Channel (SACCH)***- The SACCH is always associated with a traffic channel or a SDCCH and maps onto the same physical channel. Thus, each ARFCN systematically carries SACCH data for all of its current users. As in the USDC standard, the SACCH carries general information between the MS and BTS.

(c) ***Fast Associated Control Channels (FACCH)***-FACCH carries urgent messages, and contains essentially the same type of information as the SDCCH.A FACCH is assigned whenever a SDCCH has not been dedicated for a particular user and there is an urgent message (such as a handoff request). The FACCH gains access to a time slot by "stealing" frames from the traffic channel to which it is assigned. This is done by setting two special bits, called stealing bits, in a TCH forward channel burst. If the stealing bits are set, the time slot is known to contain FACCH data, not a TCH, for that frame.

Example of GSM call:

1. GSM to PSTN call,
2. PSTN to GSM call

- To understand how the various traffic and control channels are used, consider the case of a mobile call origination in GSM. First, the subscriber unit must be synchronized to a nearby base station as it monitors the BCH.

- By receiving the FCCH, SCH, and BCCH messages, the subscriber would be locked on to the system and the appropriate BCH. To originate a call, the user first dials the intended digit combination and presses the "send" button on the GSM phone.

- The mobile transmits a burst of RACH data, using the same ARFCN as the base station to which it is locked. The base station then responds With an AGCH message on the CCCH which assigns the mobile unit to a new channel for SDCCH connection.

- The subscriber unit, which is monitoring TS 0 of the BCH, would receive its ARFCN and *TS* assignment from the AGCH and *would* immediately tune to the new ARFCN and TS.

- This new ARFCN and TS assignment is physically the SDCCH {not the TCH). Once tuned to the SDCCH, the subscriber unit first waits for the SACCH frame to be transmitted when calls are originated from the PSTN, the process is quite similar.

- The base station broadcasts a PCH message during TS 0 within an appropriate frame on the BCH. The mobile station, locked on to that same ARFCN, detects its page and replies With an RACH message acknowledging receipt of the page.

- The base station then uses the AGCH on the CCCH to assign the mobile unit to a new physical channel for connection to the SDCCH and SACCH while the network and the serving base station are connected.
- Once the subscriber establishes timing advance and authentication on the SDCCH, the base station issues a new physical channel assignment over the SDCCH, and the TCH assignment is made.

2.11 Frame Structure for GSM

Each user transmits a burst of data during time slot assigned to it.

These data burst may have one of five specific formats.

1. Normal
2. FCCH burst
3. SCH burst
4. RACH burst
5. Dummy burst

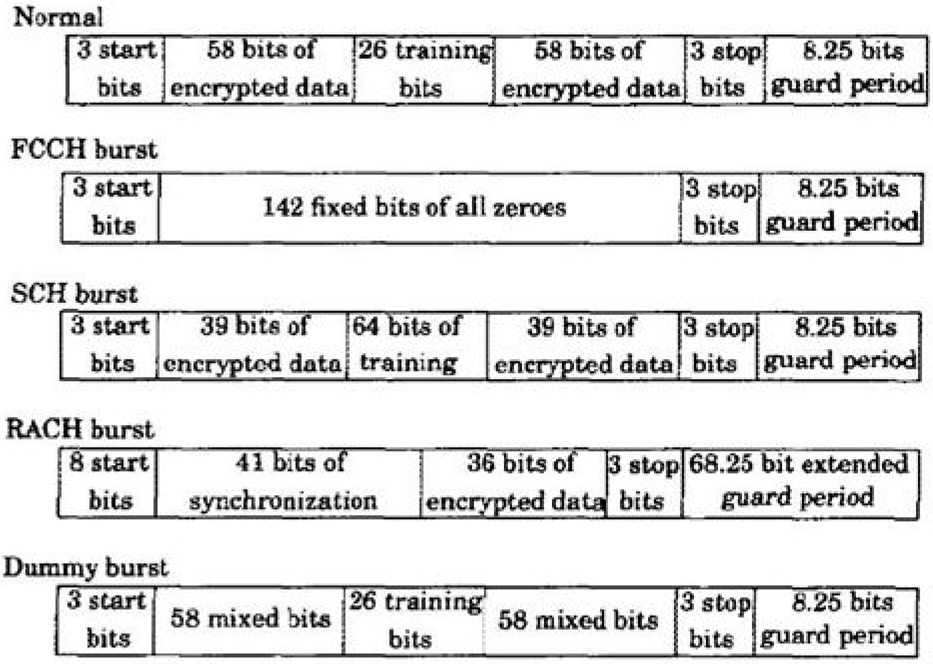


Fig. 2.4 GSM Frame Structure

- The data structure within a normal burst. It consists of 148 bits which are transmitted at a rate of 270.833333 kbps (an unused guard time of 8.25 bits is provided at the end of each burst).

- Out of the total148 bits per TS, 114 are information-bearing bits which are transmitted as two 57 bit sequences close to the beginning and end of the burst.

- The midamble consists of *a* 26 bit training sequence which allows the adaptive equalizer in the mobile or base station receiver to analyze the radio channel characteristics before decoding the user data. On either side of the midamble there are control bits called stealing flags.

- These two flags are used to distinguish whether the TS contains voice (TCH) or control (FACCH) data, both which share the same physical channel.

- During a frame, a GSM subscriber unit uses one TS to transmit, one TS to receive, and may use the six spare time slots to measure signal strength on five adjacent base stations as well as its own base station.

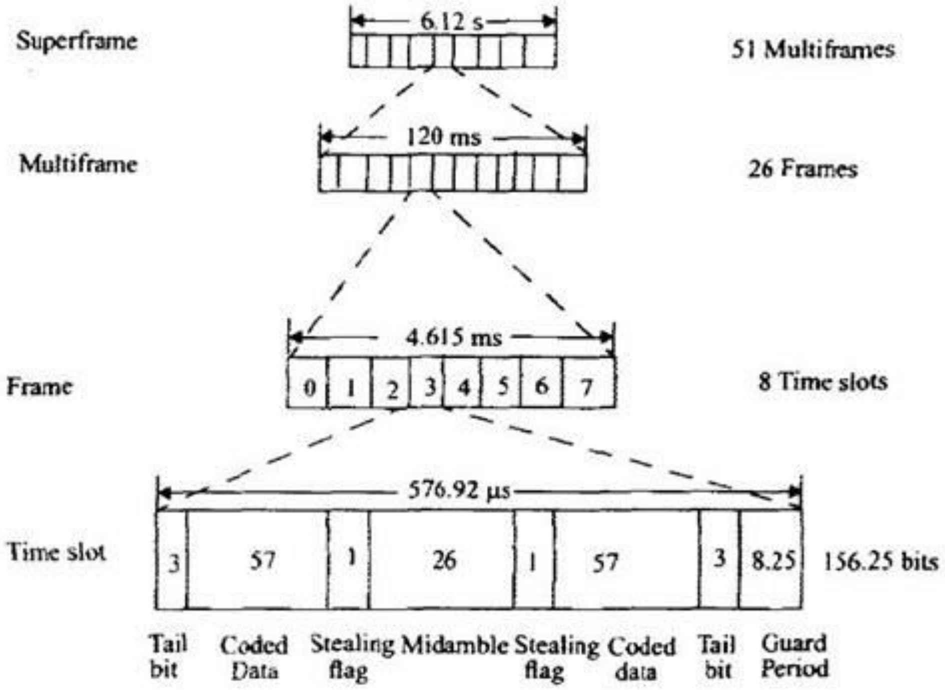


Fig. 2.5 GSM Data Structure

2.12 Signal Processing in GSM

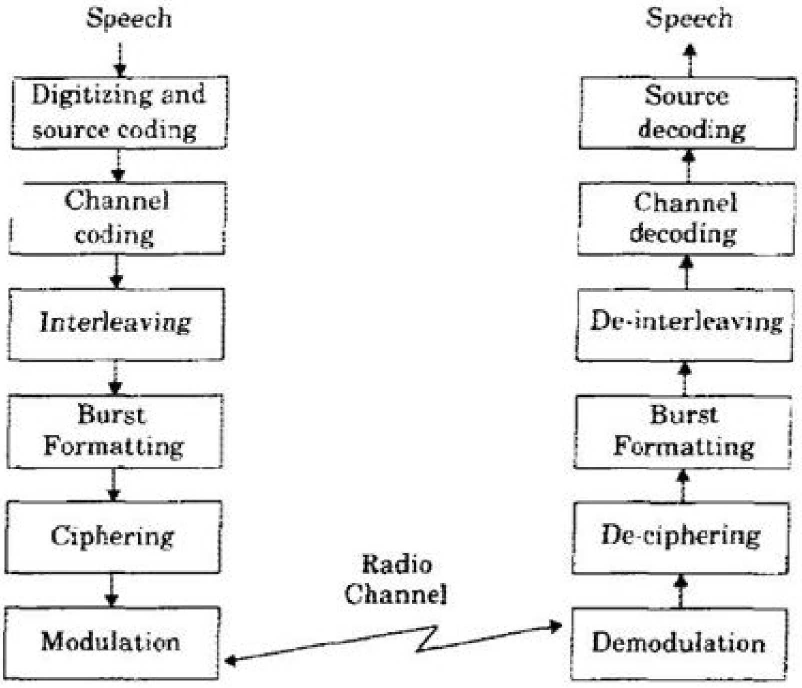


Fig. 2.6 GSM Signal Process

Speech Coding - The GSM speech coder is based on the Residually Excited Linear Predictive Coder **(RELP).** The coder provides 260 bits for each 20 ms blocks of speech, which yields a bit rate of 13 kbps. This speech coder was selected after extensive subjective evaluation of various candidate coders available in the late 1980s. Provisions for incorporating half-rate coders are included in the specifications.

TCHIFS, SACCH, and FACCH Channel Coding - The output bits of the speech coder are ordered into groups for error protection, based upon their significance in contributing to speech quality. Out of the total 260 bits **in** a frame, the most important 50 bits, called type Ia bits, have *3* parity check (CRC) bits added to them.

Channel Coding for Data Channels- The coding provided for GSM full rate data channels (TCHIF9.6) is based on handling 60 bits of user data at 5ms intervals, in accordance with the modified CCIIT V.llO modem standard.

Channel Coding for Control Channels - GSM control channel messages are defined to be 184 bits long, and are encoded using a shortened binary cyclic fire code, followed by a half-rate convolutional coder.

Interleaving - In order to minimize the effect of sudden fades on the received data, the total of 456 encoded bits within each 20 ms speech frame or control message frame are broken into eight 57 bit sub-blocks. These eight subblocks which make up a single speech frame are spread over eight consecutive TCH time slots.

Ciphering - Ciphering modifies the contents of the eight interleaved blocks through the use of encryption techniques known only to the particular mobile station and base transceiver station.

Burst Formatting - Burst formatting adds binary data to the ciphered blocks, in order to help synchronization and equalization of the received signal.

Modulation - The modulation scheme used by GSM is 0.3 GMSK where 0.3 describes the 3 dB bandwidth of the Gaussian pulse shaping filter with relation to the bit rate (e.g., $BT = 0.3$). GMSK is a special type of digital FM modulation.

Frequency Hopping- Under normal conditions, each data burst belonging to a particular physical channel is transmitted using the same carrier frequency. However, if users in a particular cell have severe multipath problems, the cell may be defined as a *hopping cell* by the network operator, in which case *slow frequency hopping* may be implemented to combat the multipath or interference effects in that cell.

Equalization - Equalization is performed at the receiver with the help of the training sequences transmitted in the midamble of every time slot. The type of equalizer for GSM is not specified and is left up to the manufacturer.

Demodulation - The portion of the transmitted forward channel signal which is of interest to a particular user is determined by the assigned TS and ARFCN.

Chapter No.03

GSM Mobility Management

3.1 MOBILITY PROCEDURES IN GSM

What are mobility procedures? For the purpose of this study, mobility procedures will be defined as the functionality required to offer and maintain communications with a mobile user at any given time and any functionality resulting as a consequence. Within GSM, authentication, ciphering and security are a integral part of the network and are intertwined with mobility functionalities. The aim of the study is to model mobility functionalities independent of the access network used. As such GSM radio access functionality is not covered here. The emphasis, as the reader will discover is, on the exchange of messages by mobility functions within the core network. The negative outcomes of mobility procedures are not discussed unless deemed significant.

3.2 LOCATION UPDATING PROCEDURE

For a mobile network to offer connectivity to a mobile user, the location of the user must be known. The procedure of a mobile terminal informing the network of its whereabouts is referred to as location updating. The request by a mobile terminal for location updating upon entry into every new cell (which may be as small as 100 meters in radius), will place undue stain on the network in terms of excessive signaling traffic. To optimize network performance and reduce signaling load, cells are grouped into *location areas*. With *location areas*, the mobile terminal is only required to update its location when it enters a new *location area*. In addition, the network requires the mobile terminal to carry out periodic location updating. The time between periodic location updates is set by the network operators and can vary from 6 minutes to a little more than a day. There are other situations (such as a VLR failure) where location updating procedure is initiated; these situations are rare compared to others and are not described here.

A user's location is stored in three different locations in the GSM network; the *subscriber identity module*, the VLR attached to the roaming MSC and the HLR. For the purposes of routing a mobile terminating call, the HLR only stores the destination of the MSC being roamed, it being the VLR that stores the *location area* the mobile terminal is currently in. This leads to two variations in the location updating procedure (illustrated in Figure 3.1):

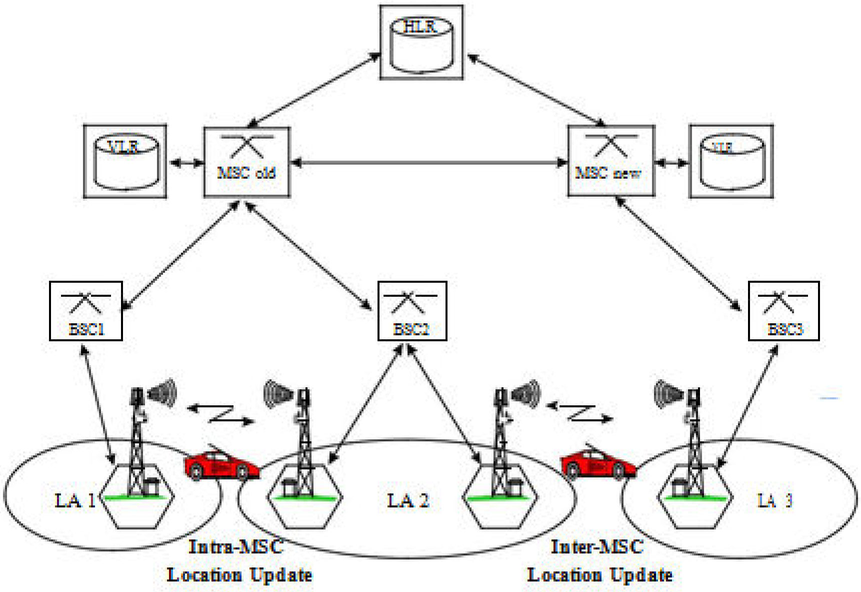


Fig. 3.1: Two location updating scenarios in GSM

- **Intra-MSC location update:** The mobile terminal moves into a new *location area* within the same MSC. In this case only the VLR needs to be informed and the HLR need not be informed as the MSC roamed is unchanged.

- **Inter-MSC location update:** The mobile terminal comes into the coverage of a new *location area* controlled by a different MSC to the one being roamed. In this case the VLR associated with the new MSC needs to be informed. The new VLR will then have to update the HLR with the new MSC's address and the old VLR will have to delete the user from its records.

3.2.1GSM location update

- GSM "location update" is a part of registration. GSM networks keep track of the location area (LA) where the MS is operating. When receiving an incoming call, the MS is paged in all cell of its current location area.

- GSM mobile do a location update when entering to new location area and at periodic interval. In addition to this, MS also updates location in ease of activation and deactivation performed by the users.

When it occurred:

Updating on entering a new location

Area:

The Location Area Identity (LAI) is broadcast in system information message and stored in mobile station memory. When a new received location area identity does not match with the previously stored location area identity, then MS does a location update.

Periodic update:

Whenever MS performs location update if reset timer T. A time has timeout value. As and when the timer expires, the MS does the location update.

Updating on deactivation and activation:

Mobile equipment does this update and send IMSI DETACH message when it is deactivated. The network marks that MS as a deactivated and does not send paging message to for MS until it is activated again. A MS send IMSI DETACH message does a location update when it is activated again.

3.2.2Mobility Database

Home location register (HLR) is a database used for mobile user information management. All permanent subscriber data are stored in this database An HLR record consists of 3 types of information:

Mobile station information

1. IMSI used by MS to access network
2. MSISDN

Location information

1. ISDN number (address) of VLR and MSC where MS resides

Service information

1. Service subscription
2. Service restrictions
3. Supplementary services

Visitor location register (VLR) is a database of the service area visited by MS. All subscriber data of an MS required for call handling and other purpose are stored in VLR.

VLR information consists of 3 parts:

Mobile station information

1. IMSI
2. MSISDN
3. TMSI

Location information

1. MSC number
2. Location area ID (LAI)

Service information

1. Subset of the service information stored in the HLR

Chapter No. 4

General Radio Packet System (GPRS)

4.1 Introduction

GPRS (General Packet Radio Service) is a packet based communication service for mobile devices that allows data to be sent and received across a mobile telephone network. GPRS is a step towards 3G and is often referred to as 2.5G. Here are some key benefits of GPRS:

Speed

GPRS is packet switched. Higher connection speeds are attainable at around 56–118 kbps, a vast improvement on circuit switched networks of 9.6 kbps. By combining standard GSM time slots theoretical speeds of 171.2 kbps are attainable. However in the very short term, speeds of 20-50 kbps are more realistic.

Always on connectivity

GPRS is an always-on service. There is no need to dial up like you have to on a home PC for instance. This feature is not unique to GPRS but is an important standard that will no doubt be a key feature for migration to 3G. It makes services instantaneously available to a device.

New and Better applications

Due to its high-speed connection and always-on connectivity GPRS enables full Internet applications and services such as video conferencing straight to your desktop or mobile device. Users are able to explore the Internet or their own corporate networks more efficiently than they could when using GSM. There is often no need to redevelop existing applications.

GSM operator Costs

GSM network providers do not have to start from scratch to deploy GPRS. GPRS is an upgrade to the existing network that sits along side the GSM network. This makes it easier to deploy, there is little or no downtime of the existing GSM network whilst implementation takes place, most updates are software so they can be administered remotely and it allows GSM providers to add value to their business at relatively small costs.

The GSM network still provides voice and the GPRS network handles data, because of this voice and data can be sent and received at the same time.

4.2Simple GPRS Technical Overview

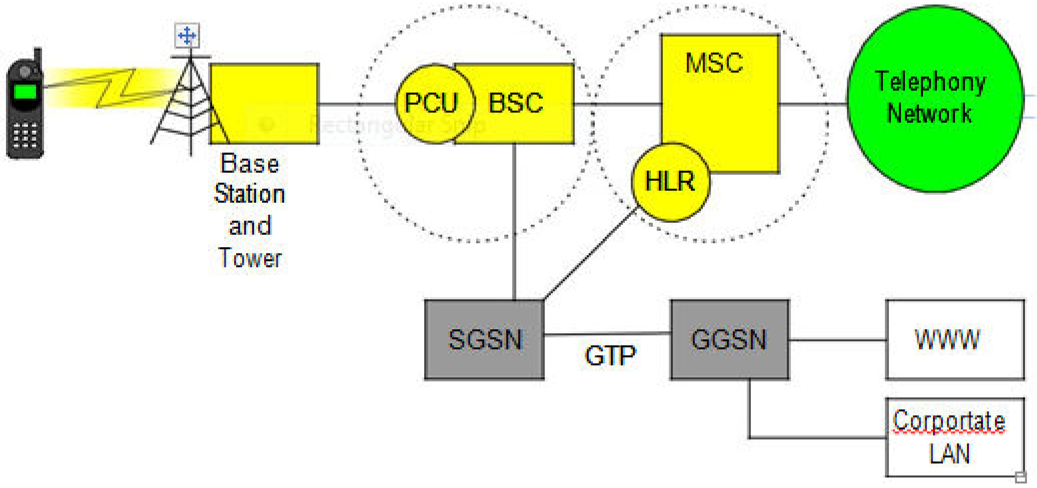


Fig. 4.1: GPRS NETWORK

As mentioned earlier GPRS is not a completely separate network to GSM. Many of the devices such as the base transceiver stations and base transceiver station controllers are still used. Often devices need to be upgraded be it software, hardware or both. When deploying GPRS many of the software changes can be made remotely.

There are however two new functional elements which play a major role in how GPRS works. The Serving GPRS Support Node (SGSN) and the Gateway GPRS support node (GGSN). These 2 nodes are new to the network with the other changes being small if any.

Before explaining what these 2 new members of our network do it is important to ask how does the network differentiate between GSM (circuit) and GPRS (packet)?

In simple terms there are in practice two different networks working in parallel, GSM and GPRS.

In any GSM network there will be several BSC’s (Base Station Controllers). When implementing GPRS software and hardware upgrade of this unit is required. The hardware upgrade consists of adding a Packet Control Unit (PCU). This extra piece of hardware differentiates data destined for the standard GSM network or Circuit Switched Data and data destined for the GPRS network or Packet Switched Data. In some cases a PCU can be a separate entity.

From the upgraded BSC there is a fast frame relay connection that connects directly to the newly introduced SGSN.

4.2.1 SGSN

The Serving GPRS Support Node, or SGSN for short, takes care of some important tasks, including routing, handover and IP address assignment.

The SGSN has a logical connection to the GPRS device. As an example, if you where in a car travelling up the M1 on a long journey and were browsing the Internet on a GPRS device, you will pass through many different cells. One job of the SGSN is to make sure the connection is not interrupted as you make your journey passing from cell to cell. The SGSN works out which BSC to “route” your connection through.

If the user moves into a segment of the network that is managed by a different SGSN it will perform a handoff of to the new SGSN, this is done extremely quickly and generally the user will not notice this has happened. Any packets that are lost during this process are retransmitted. The SGSN converts mobile data into IP and is connected to the GGSN via a tunneling protocol.

4.2.2 GGSN

The Gateway GPRS Support Node is the “last port of call” in the GPRS network before a connection between an ISP or corporate network’s router occurs. The GGSN is basically a gateway, router and firewall rolled into one. It also confirms user details with RADIUS servers for security, which are usually situated in the IP network and outside of the GPRS network.

4.2.3 Connectivity between the SGSN & GGSN

The connection between the two GPRS Support Nodes is made with a protocol called GPRS Tunneling Protocol (GTP). GTP sits on top of TCP/IP and is also responsible for the collection of mediation and billing information. GPRS is billed on per megabyte basis unlike GSM. In practice the two GSN devices may be a single unit.

4.2.4 HLR

The HLR or Home Location Register is a database that contains subscriber information, when a device connects to the network their MSISDN number is associated with services, account status information, preferences and sometimes IP addresses.

4.3 IP addressing

4.3.1 Allocating Addresses

There are 3 different ways in which a device can be assigned an IP address.

Fixed IP addressing:

Fixed IP addresses for mobile devices are not widely used due to shortages of Ipv4 addresses (see below). This information is stored in the HLR.

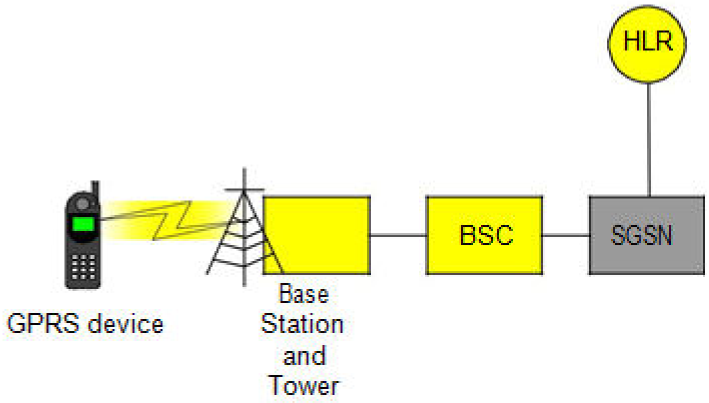


Fig. 4.2: Fixed IP Address Allocation

Dynamic IP addressing:

The second means of addressing is dynamic addressing. This is where a mobile device does not have its own IP address stored in the HLR. Instead the IP address is assigned to the GGSN domain.

The third method is also a type of dynamic IP addressing in which the IP address is assigned by RADIUS servers normally situated inside an IP network outside the mobile network, an example of this being when you dial up to an ISP from your home PC.

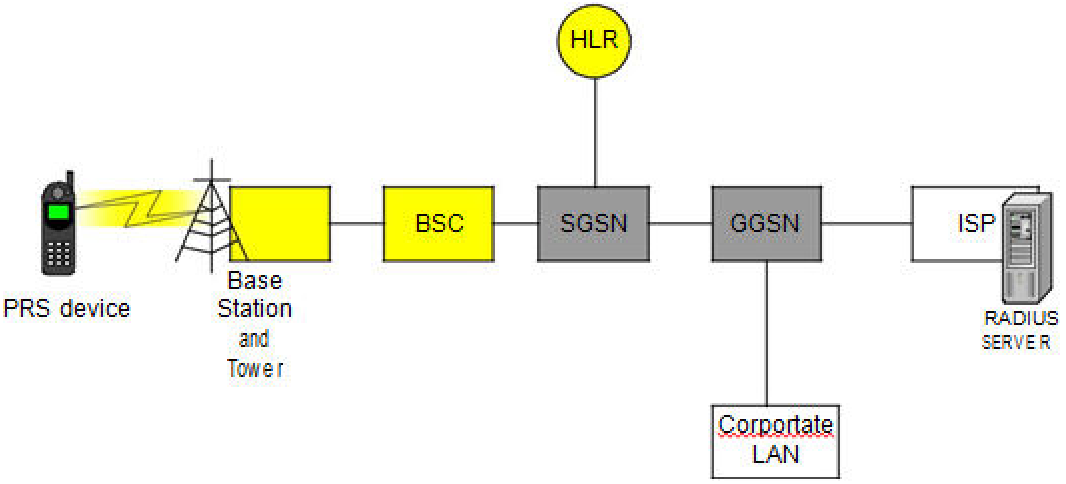


Fig. 4.3: Dynamic IP Address Allocation

4.4GPRS Handset Classes

GPRS devices are not as straightforward as you may think. There are in fact 3 different classes of device.

1. Class A

Class A terminals have 2 transceivers which allow them to send / receive data and voice at the same time. This class of device takes full advantage of GPRS and GSM. You can be taking a call and receiving data all at the same time.

2. Class B

Class B devices can send / receive data or voice but not both at the same time. Generally if you are using GPRS and you receive a voice call you will get an option to answer the call or carry on.

3. Class C

This device only allows one means of connectivity. An example would be a GPRS PCMCIA card in a laptop.

4.5 GPRS Architecture

- Following is the GPRS Architecture diagram:

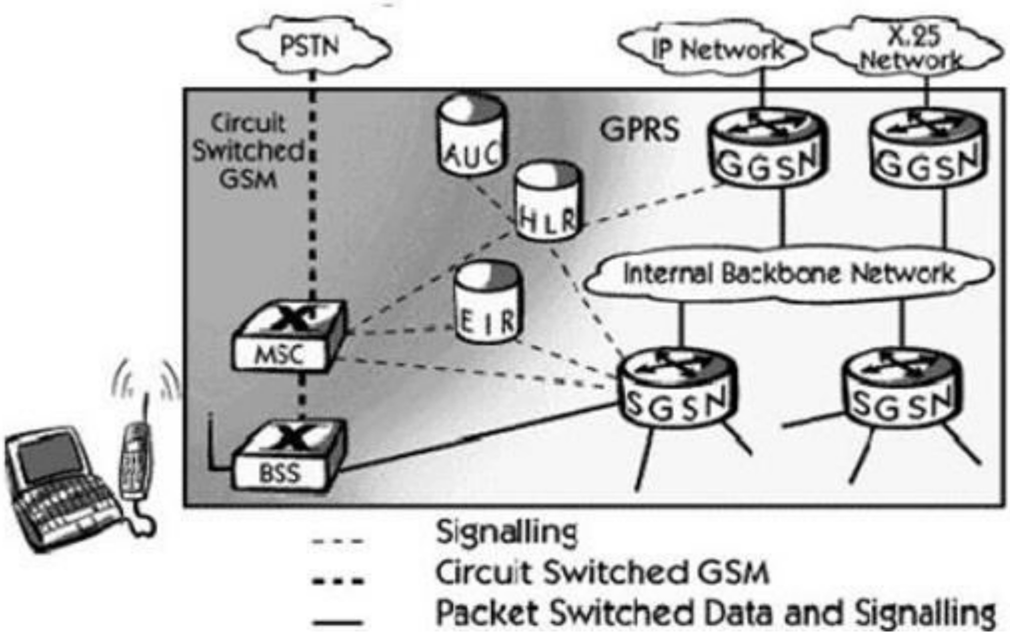


Fig. 4.4: GPRS ARCHITECTURE

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission.
- This data network overlaps a second generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps.
- Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.
- GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

4.6 GPRS Mobile Stations, Base Station subsystem

GPRS Mobile Stations

- New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data.
- A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers.
- These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

- Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade.
- The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic.
- The BTS can also require a software upgrade but typically does not require hardware enhancements.
- When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call.
- However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

4.7 GPRS Network Nodes

A GSN is a network node which supports the use of GPRS in the GSM core network. All GSNs should have a *GN* interface and support the GPRS tunneling protocol. There are two key variants of the GSN, namely Gateway and Serving GPRS support node.

1. GPRS Support Nodes,
2. Gateway GPRS Support Nodes

1. GPRS Support Nodes: Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

- The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node.

- The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

2. Serving GPRS Support Node (SGSN)

- The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

4.8 GPRS Network Operations

- Data transmission in a GPRS network requires several steps as described below in the context of the protocol layers.

- Once a GPRS mobile station is powered on, it introduces itself to the network by sending a GPRS attach request. Network access can be achieved from either the network side or the MS side of the GPRS network.

1. Attachment and Detachment Procedure
2. Mobile Management
3. Routing
4. Communicating with the IP-Networks

1. Attachment and Detachment Procedure

- In order to access the GPRS services, an MS needs to make its presence known to the network. It must register itself with an SGSN of the network.

- This is done through a GPRS attach. This operation establishes a logical link between the MS and the SGSN.

- The network checks if the MS is authorized to use the services; if so it copies the user profile from the HLR to the SGSN, and assigns a packets with external PDN after successful GPRS attach, a mobile station must apply for an address.

- This address called as PDN (packet data protocol) address. Allocation of the PDP address can be static or dynamic. In case static address the network operation permanently assigns a PDP address to the user. In dynamic allocation address change every time.

2. Mobile Management

- As a mobile station moves from one area to another, mobile management functions are used to track its location within each PLMN.
- SGSN communication with each other to update the MS location in the relevant registers.

- The mobile stations profiles are preserved in the VLR that are accessible to SGSN via the local MSC.

- A logical link is established and maintained between the mobile station and the SGSN at each PLMN.

3. Routing

- The example assumes two intra PLMN backbone networks of different PLMN.

- Intra PLMN backbone network connect GSN of the same PLMN or the same network operator.

- These are private packet based networks of the GPRS network provider; for example Airtel GSN in Mumbai connecting to Airtel GSN in Delhi through a private data network.

- GPRS mobile station located in PLMN1 send IP packets to a host connected to the IP network e.g to a web server connected to the internet.

4. Communicating with the IP network

- A GPRS network can be interconnected with Internet or a corporate internet.

- GPRS supports both IPv4 and IPv6. From an external IP networks point of view, the GPRS network looks like any other IP sub-network, and the GGSN looks like a usual IP router.

- The IP address is taken from the address space of the GPRS operator maintained by a DHCP server.

4.9 Data Services in GPRS

A wide range of corporate and consumer applications are enabled by GPRS services. A user is likely to use either of two modes of GPRS network.

1. Application Mode
2. Tunneling Mode

Application Mode:-

- In this mode user will be using the GPRS mode phone to access the applications running on the phone itself.
- The phone here acts as the end user device. All GPRS phones have WAP browser as an embedded application.
- This browser allows browsing of WAP sites. The device operating executed environments supported are Symbain and J2ME.
- Application can be developed in C/C++ or java.

Tunneling Mode:-

- This mode is for mobile computing where the user will use the GPRS interface as an access to the network.

- The end user device will be a large footprint device like laptop computer or small footprint device like PDA.

- The mobile phone will be connected to the device and used as modem to access the wireless data network.

Also data services in GPRS

1. GPRS handsets
2. Device type
3. Bearers in GPRS

GPRS handsets

A GPRS terminal can be one of three classes: A, B or C. A Class A terminal supports GPRS data and other GSM services such as a MMS and voice simultaneously. This includes Simultaneous attach, activation, monitor and traffic. As such, a Class A terminal can make or receive calls on two services simultaneously. In the presence of circuit switched services, GPRS virtual circuits will be held or place on busy rather than being cleared. SMS is supported in Class A terminal like GSM, a SMS can be received while a voice or data call in a progress.

Applications and Limitations of GPRS

Applications:

1. **Mobility -** The ability to maintain constant voice and data communications while on the move.

2. **Immediacy -** Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.

3. **Localization -** Allows subscribers to obtain information relevant to their current location.

4. **Communications -** E-mail, fax, unified messaging and intranet/internet access,

   etc.

5. **Value-added services -** Information services and games, etc.

6. **E-commerce -** Retail, ticket purchasing, banking and financial trading, etc.

7. **Location-based applications -** Navigation, traffic conditions, airline/rail schedules and location finder, etc.

8. **Vertical applications -** Freight delivery, fleet management and sales-force automation.

9. **Advertising -** Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

Limitations:

1. **Limited Cell Capacity for All Users**

GPRS does impact a network's existing cell capacity. There are only limited radio resources that can be deployed for different uses

2. **Speeds Much Lower in Reality**

Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight timeslots without any error protection.

3. **Transit Delays**

GPRS packets are sent in all different directions to reach the same destination. This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link.

Basic characteristics of GPRS

General Packet Radio Service (GPRS) enabled networks offer "always-on", higher capacity, Internet-based content and packet-based data services. This enables services such as colour Internet browsing, e-mail on the move, powerful visual communications, multimedia messages and location-based services.

1. GPRS main features

SPEED:

Theoretical maximum speeds of up to 171,2 kilobits per second (kbps) are achievable with GPRS using all eight timeslots at the same time. This is about three times as fast as the data transmission speeds possible over today's fixed telecommunications networks and ten times as fast as current Circuit Switched Data services on GSM networks.

IMMEDIACY:

GPRS facilitates instant connections whereby information can be sent or received immediately as the need arises, subject to radio coverage. No dial-up modem connection is necessary. This is why GPRS users are sometimes referred to be as being "always connected". Immediacy is one of the advantages of GPRS (and SMS) when compared to Circuit Switched Data. High immediacy is a very important feature for time critical applications such as remote credit card authorization where it would be unacceptable to keep the customer waiting.

NEW/BETTER APPLICATIONS:

GPRS facilitates several new applications that have not previously been available over GSM networks due to the limitations in speed of Circuit Switched Data (9,6 kbps) and message length of the Short Message Service (160 characters). GPRS will fully enable many Internet and co-operative applications from web browsing to interacting with broadcast content.

2. SERVICE ACCESS:

To use GPRS, users specifically need:

- A mobile phone or terminal that supports GPRS;
- A subscription to a mobile telephone network that supports GPRS;
- Use of GPRS must be enabled for that user. Automatic access to the GPRS may be allowed by some mobile network operators, others will require a specific opt-in;
- Procedures for how to send and/ or receive GPRS information using their specific model of mobile phone, including software and hardware configuration;
- A destination to send or receive information through GPRS. Whereas with SMS this was often another mobile phone, in the case of GPRS, it is likely to be an Internet or IP address.

3. Key network features of GPRS

PACKET SWITCHING:

GPRS involves overlaying a packet based air interface on the existing circuit switched GSM network. This gives the user an option to use a packet-based data service.

SPECTRUM EFFICIENCY:

Packet switching means that GPRS radio resources are used only when users are actually sending or receiving data. GPRS improves the peak time capacity of a GSM network since it allocates scarce radio resources more efficiently by supporting virtual connectivity.

INTERNET AWARE:

For the first time, GPRS fully enables Mobile Internet functionality by allowing interworking between the existing Internet and the new GPRS network. Any service that is used over the fixed Internet today - File Transfer Protocol (FTP), web browsing, chat, e-mail, telnet - will be available over the mobile network via GPRS. Because it uses the same protocols, the GPRS network can be viewed as a sub-network of the Internet with GPRS capable mobile phones being viewed as mobile hosts. This means that each GPRS terminal can potentially have its own IP address and will be addressable as such.

SUPPORTS TDMA AND GSM:

It should be noted right that the General Packet Radio Service is not only a service designed to be deployed on mobile networks that are based on the GSM digital mobile phone standard. The IS-

136 Time Division Multiple Access (TDMA) standard, popular in North and South America, will also support GPRS. This follows an agreement to follow the same evolution path towards third generation mobile phone networks concluded in early 1999 by the industry associations that support these two network types.

4. Limitations of GPRS

LIMITED CELL CAPACITY FOR ALL USERS:

GPRS does impact a network's existing cell capacity. There are only limited radio resources that can be deployed for different uses - use for one purpose precludes simultaneous use for another. For example, GSM voice and GPRS calls both use the same network resources. The extent of the impact depends upon the number of timeslots, if any, that are reserved for exclusive use of GPRS. However, GPRS does dynamically manage channel allocation and allow a reduction in peak time signaling channel loading by sending short messages over GPRS channels instead.

SPEEDS PRACTICALLY LOWER IN REALITY:

Achieving the theoretical maximum GPRS data transmission speed of 172,2 kbps would require a single user taking over all eight timeslots without any error protection. Clearly, it is unlikely that a network operator will allow all timeslots to be used by a single GPRS user. Additionally, the initial GPRS terminals are expected be severely limited - supporting only one, two or three timeslots. The bandwidth available to a GPRS user will therefore be severely limited. As such, the theoretical maximum GPRS speeds should be checked against the reality of constraints in the networks and terminals. The reality is that mobile networks are always likely to have lower data transmission speeds than fixed networks.

5. GPRS Multisport Classes

Multislot classes are product dependent, and determine the maximum achievable data rates in both the uplink and downlink directions. Written as (for example) 3 + 1 or 2 + 2, the first number indicates the amount of downlink timeslots (what the mobile phone is able to receive from the network).The second number indicates the amount of uplink timeslots (how many timeslots the mobile phone is able to transmit).The active slots determine the total number of slots the GPRS device can use simultaneously for both uplink and downlink communications.

Multislot Class	Downlink Slots	Uplink Slots	Active Slots
1	1	1	2
2	2	1	3
3	2	2	3
4	3	1	4
5	2	2	4
6	3	2	4
7	3	3	4
8	4	1	5
9	3	2	5
10	4	2	5
11	4	3	5
12	4	4	5

TABLE 4.1

The class indicates the mobile phone capabilities.

Class A:

Class A mobile phones can be connected to both GPRS and GSM services simultaneously.

Class B:

Class B mobile phones can be attached to both GPRS and GSM services, using one service at a time. Class B enables making or receiving a voice call, or sending/receiving an SMS during a GPRS connection. During voice calls or SMS, GPRS services are suspended and then resumed automatically after the call or SMS session has ended.

Class C:

Class C mobile phones are attached to either GPRS or GSM voice service. You need to switch manually between services.

Introduction to 3G and 4G technologies

3G Technology:-

- Several telecommunications companies market wireless mobile Internet services as *3G*, indicating that the advertised service is provided over a 3G wireless network.

- Services advertised as 3G are required to meet IMT-2000 technical standards, including standards for reliability and speed (data transfer rates).

- To meet the IMT-2000 standards, a system is required to provide peak data rates of at least 200 kbit/s (about 0.2 Mbit/s).

- However, many services advertised as 3G provide higher speed than the minimum technical requirements for a 3G service. Recent 3G releases , often denoted 3.5G and 3.75G, also provide mobile broadband access of several M bits/s to Smartphone’s and mobile modems in laptop computers.

4G Technology:-

- 4G, short for fourth generation, is the fourth generation of mobile telecommunications technology, succeeding 3G.

- A 4G system must provide capabilities defined by ITU in IMT Advanced. Potential and current applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, 3D television, and cloud computing.

- Two 4G candidate systems are commercially deployed: the Mobile WiMAX standard (first used in South Korea in 2007), and the first-release Long Term Evolution (LTE) standard (in Oslo, Norway, and Stockholm, Sweden since 2009). It has however been debated if these first-release versions should be considered to be 4G or not, as discussed in the technical definition section below.

The following standards are typically branded 3G:

1. **UMTS**

2. **CDMA 2000**

UMTS (Universal Mobile Telecommunications System):-

- The Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system for networks based on the GSM standard.

- Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing CDMA One technology.

- UMTS uses wideband code division multiple access (W-CDMA) radio access technology to offer greater spectral efficiency and bandwidth to mobile network operators.

- UMTS specifies a complete network system, which includes the radio access network (UMTS Terrestrial Radio Access Network, or UTRAN), the core network (Mobile Application Part, or MAP) and the authentication of users via SIM (subscriber identity module) cards.

- The UMTS system, first offered in 2001, standardized by 3GPP, used primarily in Europe, Japan, China (however with a different radio interface) and other regions predominated by GSM 2G system infrastructure.

- The cell phones are typically UMTS and GSM hybrids. Several radio interfaces are offered, sharing the same infrastructure:

- The original and most widespread radio interface is called W-CDMA.

- The TD-SCDMA radio interface was commercialized in 2009 and is only offered in China.

- The latest UMTS release, HSPA+, can provide peak data rates up to 56 Mbit/s in the downlink in theory (28 Mbit/s in existing services) and 22 Mbit/s in the uplink.

CDMA 2000:-

- CDMA 2000(also known as C2K or IMT Multi-Carrier(IMT-MC) is a family of 3G mobile technology standards for sending voice, data and signaling data between mobile phones and cell sites

- It is developed by 3GPP as a backwards –compatible successor to second generation CDMA one (IS-95) set of standards and used especially in North America and South Korea

- CDMA2000 compares to UMTS, a competing set of 3G standards, which is developed by 3GPP and used in Europe, Japan, and China. The name CDMA2000 denotes a family of standards that represent the successive, evolutionary stages of the underlying technology.

These are:

- Voice: CDMA2000 1xRTT, 1X Advanced

- Data: CDMA2000 1xEV-DO (Evolution-Data Optimized): Release 0, Revision A, Revision B, Ultra Mobile Broadband (UMB)

Chapter No-5

Mobile Security

5.1KEY FEATURES of Mobile Security

Malware Scanning

Industry-leading anti-malware technology detects and blocks viruses, worms, Trojans, spyware, and evolving malicious mobile code on handheld units and storage cards.

Anti-spam for SMS Messages

Trend Micro Mobile Security provides flexible anti-spam options, including lists for both approved and blocked senders, as well as the ability to block short text and multimedia messages from unknown senders.

Web Threat Defense

Unique Web reputation technology prevents threats from entering smartphones and PDAs during Internet surfing.

Anti-theft Security

Allows device owners to delete stored information remotely in case the unit is stolen, lost, or compromised. It will also lock the device if unauthorized users attempt to remove or change the installed SIM card.

Data Protection from Accidental Loss

Password protection prevents unauthorized access of information and minimizes accidental data loss.

Automatic and Manual Scanning

Trend Micro Mobile Security performs automatic, real-time scans, and allows users to initiate manual scans to check for viruses in individual files, file archives, and applications.

Flexible Updates

Trend Micro Mobile Security delivers updated pattern files to mobile devices via wireless data connection or by synchronizing with a PC via ActiveSync.

Parental Controls

Parental Controls allow blocking of outgoing calls or SMS messages to undesirable numbers. Logs and parental control settings are protected by a security password.

5.2 Threat Vectors Introduced by Mobile

The use of Mobile devices to enhance enterprise productivity, organizations are being exposed to a variety of information security risks and threats. Threats introduced by mobile can be grouped in to three categories:

1) Device based threat vectors

Mobile devices enable end-users to perform a variety of business-related tasks such as receiving email and accessing, editing and sharing corporate content via a variety of productivity apps. As a result, mobile devices store a significant amount of sensitive data. This data can be compromised in a variety of ways due to:

- Always-on connectivity which could allow unauthorized parties to access business data.
- Software vulnerabilities that allow "jailbreak" or "rooting" of devices, compromising data security.
- Portable form-factor making the devices susceptible to theft and misplacement.

2) Network based threat vectors

The always-on model requires mobile devices to be constantly connected to the internet. As a result, end-users might often rely on untrusted public networks enabling malicious parties to access and intercept transmitted data using

- Rogue access points

- Wi-Fi sniffing tools

- Sophisticated Man-in-the-Middle (MitM) attacks

3) User based threat vectors

Mobile empowers end-users. While this is great for user-choice, well-meaning end-users often indulge in risky behaviors that could compromise business data. Examples of risky behaviors include:

- Using un-approved cloud-based apps to share and sync data

- Using un-approved productivity apps that maintain copies of corporate data

- Jail breaking/ rooting devices to bypass security controls

- Using malicious apps from un-approved app-stores

- Exposing business data with malicious intent

5.3 Countermeasures for data loss prevention on Mobile

Implementing data loss prevention on mobile devices requires a layered security approach. This layered security approach can be implemented using the controls listed below:

1) Secure operating system architecture

2) Authentication

3) Remote wipe

4) Encryption

5) Data sharing

6) Network security

7) Application lifecycle management

8) Secure browsing

5.4 Take Steps to Protect Your Mobile Phone

Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones. However, following best practices regarding mobile phone security can reduce the likelihood or consequences of an attack.

- **When choosing a mobile phone, consider its security features.** Ask the service provider if the device offers file encryption, the ability for the provider to find and wipe the device remotely, the ability to delete known malicious apps remotely, and authentication features such as device access passwords. If you back up your phone data to a PC, look for an option to encrypt the backup. If you plan to use the device for VPN access, as some users do to access work networks, ask the provider if the device supports certificate-based authentication.

- **Configure the device to be more secure.** Many smartphones have a password feature that locks the device until the correct PIN or password is entered. Enable this feature, and choose a reasonably complex password. Enable encryption, remote wipe capabilities, and antivirus software if available.

- **Configure web accounts to use secure connections.** Accounts for certain websites can be configured to use secure, encrypted connections (look for “HTTPS” or “SSL” in account options pages). Enabling this feature deters attackers from eavesdropping on web sessions. Many popular mail and social networking sites include this option.

- **Do not follow links sent in suspicious email or text messages.** Such links may lead to malicious websites.

- **Limit exposure of your mobile phone number.** Think carefully before posting your mobile phone number to a public website. Attackers can use software to collect mobile phone numbers from the web and then use those numbers to target attacks.

- **Carefully consider what information you want stored on the device.** Remember that with enough time, sophistication, and access to the device, any attacker could obtain your stored information.

- **Be choosy when selecting and installing apps.** Do a little research on apps before installing them. Check what permissions the app requires. If the permissions seem beyond what the app should require, do not install the app; it could be a Trojan horse, carrying malicious code in an attractive package.

- **Maintain physical control of the device, especially in public or semi-public places.**
  The portability of mobile phones makes them easy to lose or steal.

- **Disable interfaces that are not currently in use, such as Bluetooth, infrared, or Wi-Fi.** Attackers can exploit vulnerabilities in software that use these interfaces.

- **Set Bluetooth-enabled devices to non-discoverable.** When in discoverable mode, your Bluetooth-enabled devices are visible to other nearby devices, which may alert an attacker or infected device to target you. When in non-discoverable mode, your Bluetooth-enabled devices are invisible to other unauthenticated devices.

- **Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots.** Attackers can create phony Wi-Fi hotspots designed to attack mobile phones and may patrol public Wi-Fi networks for unsecured devices. Also, enable encryption on your home Wi-Fi network.[11]

- **Delete all information stored in a device prior to discarding it.** Check the website of the device's manufacturer for information about securely deleting data. Your mobile phone provider may also have useful information on securely wiping your device.
- **Be careful when using social networking applications.** These apps may reveal more personal information than intended, and to unintended parties. Be especially careful when using services that track your location.

- **Do not "root" or "jailbreak" the device.** Third-party device firmware, which is sometimes used to get access to device features that are locked by default, can contain malicious code or unintentional security vulnerabilities. Altering the firmware could also prevent the device from receiving future operating system updates, which often contain valuable security updates and other feature upgrades.

5.5 Act Quickly if Your Mobile Phone or PDA Is Stolen

- **Report the loss to your organization and/or mobile service provider.** If your phone or PDA was issued by an organization or is used to access private data, notify your organization of the loss immediately. If your personal phone or PDA was lost, contact your mobile phone service provider as soon as possible to deter malicious use of your device and minimize fraudulent charges.

- **Report the loss or theft to local authorities.** Depending on the situation, it may be appropriate to notify relevant staff and/or local police.

- **Change account credentials.** If you used your phone or PDA to access any remote resources, such as corporate networks or social networking sites, revoke all credentials that were stored on the lost device. This may involve contacting your IT department to revoke issued certificates or logging into websites to change your password.

- **If necessary, wipe the phone.** Some mobile service providers offer remote wiping, which allows you or your provider to remotely delete all data on the phone.

5.6 Implementation

After the mobile device solution has been designed, the next step is to implement and test a pilot of the design, before putting the solution into production. Aspects of the solution that should be evaluated for each type of mobile device include the following:

Connectivity: Users can establish and maintain connections from the mobile device to the organization from the locations they are expected to use. Users can connect to all of the organization's resources that they are permitted to and cannot connect to any other organization resources.

Protection: Information stored on the mobile device and communications between the mobile device and the organization are protected in accordance with the established requirements.

Authentication: Authentication is required and cannot be readily compromised or circumvented. All device, user, and domain authentication policies are enforced.

Applications: The applications to be supported by the mobile device solution function properly. All restrictions on installing applications are enforced. All restrictions on uninstalling applications (such as enterprise mobile device management software) are enforced.

Management: Administrators can configure and manage all components of the solution effectively and securely. The ease of deployment and configuration is particularly important. Another concern is the ability of users to alter device/client software settings, which could weaken mobile device security.

Logging: The mobile device solution logs security events in accordance with the organization's policies. See NIST SP 800-92, *Guide to Computer Security Log Management*, for additional information on logging. Note that the security logging capabilities of mobile devices vary widely.

Performance: All components of the solution provide adequate performance during normal and peak usage. It is important to also consider the performance of intermediate devices, such as routers and firewalls.

Security of the Implementation: The mobile device implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. Organizations with high security needs may choose to perform extensive vulnerability assessments against the mobile device solution components. At a minimum, all components should be updated with the latest available patches and configured following sound security practices. The organization should also take basic measures to prevent the user from circumventing the device's security features. Also, jail broken or rooted mobile devices should be automatically detected to prohibit their use, for cases in which detection is feasible.

Default Settings: On a per-OS version basis, implementers should carefully review the default values for each mobile device setting and alter the settings as necessary to support security requirements. Implementers should also ensure that the mobile device solution does not unexpectedly "fall back" to insecure default settings for interoperability or other reasons.

Information security

- In any defense system, we need to know our enemy. We also need to determine possible areas –weak points, vulnerabilities where the enemy may attack.

- We need to build a defense system around these vulnerabilities. To build an information security system, we need answer the following questions.
- Who is enemy?
- What are the vulnerabilities? What are the weak links in the system?
- What needs special protection?
- To protect our assets from attack.
- Etc.

5.7Attacks

A security system is a system to defend our assets attacks. In the physical world these attacks are carried out the weak points in the defense system.
Attacks on dynamic assets can be the following types.

1. **Interception**
2. **Modification**
3. **Fabrication**
4. **Interruption**

Interception

An unauthorized party gaining access to an asset will be part of this attack. This is an attack on confidentiality like unauthorized copying of files or tapping a conversation between parties. Some of the sniffing attacks fall in this category.

Modification

An unauthorized party gaining control of an asset and tampering with it is party of this attack. This is an attack on integrity like changing the content of a message being transmitted through the network. Different types of man in the middle attacks are part of this type of attack.

Fabrication

An unauthorized party inserts counterfeited objects into the system for example impersonating someone and inserting a spurious message in a network.

Interruption

An asset is destroyed or made unusable. This is an attack on availability. This attack can be on a static asset or dynamic asset. Example could be cutting a communication line or making the router so busy that a user cannot use a server in a network. These are all Denial of service attack.

Attacks on static assets can be of the following types.

1. **Virus and worms**
2. **Denial of service**
3. **Intrusion**
4. **Replay attack**
5. **Buffer overflow attacks**
6. **Trapdoor attacks**

Virus and worms

These are a type of program that replicates and propagates from one system to another.

Denial of service

These are attacks on the system to prevent legitimate users from using the service.

Intrusion

These are people or software, which enter into computer system and perform function without the knowledge of the owner of the asset.

Replay attack

In a replay attack the opponent passively captures the data without trying to analyse the content.

Buffer overflow attacks

In a buffer overflow attack, the vulnerability of an executable program is exploited to force a stack overflow condition, inducing the program counter of the process to change.

5.8 Component of Information Security

Information security is an art of keeping the message secret in to encrypt and hide it from others getting to know it. The components are: (CIANATA)

1. Confidentiality
2. Integrity
3. Availability
4. Non- repudiation
5. Authorization
6. Trust
7. Accounting

1. Confidentiality: It is the property where the information is kept secret so that unauthorized persons cannot get at the information. It is ensured through Encryption of data.

2. Integrity: Integrity is achieved by adding additional information into a message. It is done through checksums, message digests or digital signature. The receiver of the message checks this extra information to verify whether the message has been tampered.

3. Authentication is a process by which we validate the identity of the parties involved in a transaction.

4. In Non – repudiation, we identify the identity of these parties beyond any point of

doubt. Nonrepudiation does not allow the sender of the message to refute the claim of not sending that message

5. Availability: Media management is part of the larger security framework. It is essential to ensure availability of service.

6. Trust: Trust involves developing a security policy, assigning credentials to entities, verifying that credentials fulfill the policies

7. Accounting: It is the process by which usage of service is metered. Based on the usage, the service provider collects the fees either directly from the customer or through home network. This will be true even if the user is roaming in a foreign network and using the services in a foreign network

5.9 Security Techniques and Algorithms-

Streams Ciphering and Block Ciphering

- A **stream cipher** is an encryption algorithm that encrypts 1 bit or byte of plaintext at a time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.

- A **block cipher** is an encryption algorithm that encrypts a fixed size of n-bits of data - known as a block - at one time. The usual sizes of each block are 64 bits, 128 bits, and 256 bits. So for example, a 64-bit block cipher will take in 64 bits of plaintext and encrypt it into 64 bits of cipher text. In cases where bits of plaintext are shorter than the block size, padding schemes are called into play. Majority of the symmetric ciphers used today are actually block ciphers. DES, Triple DES, AES, IDEA, and Blowfish are some of the commonly used encryption algorithms that fall under this group.

Symmetric Key Cryptography

Symmetric encryption, also referred to as conventional encryption or single key encryption was the only type of encryption in use prior to the development of public-key encryption.

1. **Plaintext**: This is the original intelligible message or data that is fed to the algorithm as input.

2. **Encryption algorithm**: The encryption algorithm performs various substitutions and permutations on the plaintext (see the examples of the substitution and permutation ciphers in Lecture 8).

3. **Secret Key**: The secret key is also input to the encryption algorithm. The exact substitutions and permutations performed depend on the key used, and the algorithm will produce a different output depending on the specific key being used at the time.

4. **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the key. The ciphertext is an apparently random stream of data, as it stands, is unintelligible.

5. **Decryption Algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Public Key Cryptography

- Public-key cryptography is a radical departure from all that has gone before.

- Right up to modern times all cryptographic systems have been based on the elementary tools of substitution and permutation.

- However, public-key algorithms are based on mathematical functions and are asymmetric in nature, involving the use of two keys, as opposed to conventional single key encryption. Several misconceptions are held about p-k: 1. that p-k encryption is more secure from cryptanalysis than conventional encryption. In fact the security of any system depends on key length and the computational work involved in breaking the cipher.

- That p-k encryption has superseded single key encryption. This is unlikely due to the increased processing power required.

- That key management is trivial with public key cryptography, this is not correct.

Security Frame Works for Mobile Environment-

3GPP: It is 3rd Generation Partnership Project.

- 3rd Generation Partnership Project (3GPP) is a collaborative project aimed at developing globally acceptable specifications for third generation (3G) mobile systems.

- It is collaboration between groups of telecommunications associations, to make a globally applicable third generation (3G) mobile phone system.

- 3GPP Specifications are also referred to as UTRAN, UMTS (in Europe) and FOMA (in Japan).

- The telecommunications standards bodies that make up the 3GPP are known as Organizational Partners (OP) and those are:

- Japan‟s Association of Radio Industries and Businesses (ARIB)
- Japan‟s Telecommunications Technology Committee (TTC),
- China Communications Standards Association (CCSA),
- South Korea‟s Telecommunications Technology Association (TTA),
- European Telecommunications Standards Institute (ETSI), and

- Alliance for Telecommunications Industry Solutions (ATIS).

The Four Technical Specification Groups (TSG) in 3GPP are:

- Radio Access Networks (RAN),
- Service and Systems Aspects (SA),
- Core Network and Terminals (CT) and
- GSM EDGE Radio Access Networks (GERAN).

5.10 Smart Card Security:

What is smart card?

Smart card is called „smart" because it contains a computer chip. Indeed, smart card is often referred to as „chip card" or „integrated circuit card". It provides not only memory capacity, but computational capability as well. The self-containment of smart card makes it resistant to attack, as it does not need to depend upon potentially vulnerable external resources. Because of this characteristic, smart cards are often used in different applications, which require strong security protection and authentication.

Where are smart cards used?

There are different types of smart cards used in various application scenarios like: Smart card can act as an identification card, which is used to prove the identity of the card holder. It can also be a medical card, which stores the medical history of a person. Furthermore, the smart card can be used as a credit/debit bank card which allows off-line transactions. All of these applications require sensitive data to be stored in the card, such as biometrics information of the card owner, personal medical history, and cryptographic keys for authentication, etc.

In same way, one more example of smart card is SIM in mobile phone. SIM card (also known as a subscriber identity module) is a smart card with a microprocessor and it consists of the following modules:

- CPU Program memory (ROM)
- Working memory (RAM)
- Data memory (EPROM or E2PROM)

- Serial communication module

- SIM stores subscriber data that includes user identity, network authorization data, personal security keys, contact lists and stored text messages.

Smart Card Security:

Factors which make SIM secure are:

1. Cryptographic algorithm

The presence of cryptographic algorithm and secret key in SIM card makes the SIM card secure. The most sensitive information of SIM card is the cryptographic algorithm A3, A8, secret Ki, PIN, PUK and Kc. A3, A8 algorithm were written into the SIM card in the producing process, and most people could not read A3, A8 algorithm. HN code could be settled by the phone owners. PUK code is held by the operator. Kc was derived in the process of encryption from Ki. Many of SIMS have RSA, DES, 3DES cryptographic algorithms implemented.

- **Secret key:**

  PIN and PUK

  PIN – Personal Identification Number.

  2 PINs exist (PIN1 and PIN2).

  Limited attempts on PIN access.

  - PUK-PIN Unblocking Code.

  - Resetting PUK, resets PIN and the attempt counter.

- Too many attempts on PUK blocks use permanently.

2. SIM files system:

- SIM is organized in a hierarchical tree structure; it consists of the following three types of elements: Master File (MF).
- Dedicated File (DF).
- Elementary File (EF).

These file systems have stringent security controls. These files are even protected through password known to user or operator.

Multifactor Security

Multifactor security implies to a system that requires more than one method of authentication from independent categories of credentials to verify the user"s identity for a login or other transaction. Multifactor Security can be a combination of any of the following factors:

1. What You Know

The idea here is that you know a secret often called a password that nobody else does. Thus, knowledge of a secret distinguishes you from all other individuals. And the authentication system simply needs to check to see if the person claiming to be you knows the secret. Password Pass Phrase PIN Answer to some personal question Sequence of a Number Predetermined events

2. What You Have

Instead of basing authentication on something a principal knows and can forget, maybe we should base it on something the principal has. Various token/card technologies support authentication along these lines. For all, 2-factor authentication becomes important an authentication process that involves 2 independent means of authenticating the principal. So, we might require that a principal not only possess a device but also know some secret password (often known as a PIN, or personal identification number). Without 2-factor authentication, stealing the device would allow an attacker to impersonate the owner of the device; with 2-factor authentication, the attacker would still have another authentication burden to overcome.

Magnetic strip card. (e.g. Credit card) One serious problem with these cards is that they are fairly easy to duplicate. It only costs about $50 to buy a writer, and it's easy to get your hands on cards to copy them. To get around these problems, banks implement 2-factor authentication by requiring knowledge of a 4 to 7 character PIN whenever the card is used.

Proximity card or RFID. These cards transmit stored information to a monitor via RF. There is currently a debate in this country as to the merits of using RF proximity cards (RFID tags) for identification of people and products.

Challenge/Response cards and Cryptographic Calculators. These are also called smart cards and perform some sort of cryptographic calculation. Sometimes the card will have memory, and sometimes it will have an associated PIN. A smart card transforms the authentication problem for humans, because we are no longer constrained by stringent computational and storage limitations. Unfortunately, today's smart cards are vulnerable to power-analysis attacks.

3. What You Are

Since people forget things and lose things, one might contemplate basing an authentication scheme for humans on something that a person is. After all, we recognize people we interact with not because of some password protocol but because of how they look or how they sound

--- "something they are". Authentication based on "something you are" will employ behavioral and physiological characteristics of the principal. These characteristics must be easily measured accurately and preferably are things that are difficult to spoof. For example, we might use

Chapter No. 6

Mobile Operating System

6.1 MOBILE OPERATING SYSTEMS

A mobile operating system (Mobile OS) is a software platform on top of which other programs called application programs, can run on mobile devices such as personal digital assistant (PDA) , tablets, cellular phones, smartphones and so on. Over the years, Mobile OS design has experienced a three-phase evolution: from the PC-based operating system to an embedded operating system to the current smartphone-oriented operating system in the past decade. Throughout the process, Mobile OS architecture has gone from complex to simple to something in-between. The evolution process is naturally driven by the technology advancements in hardware, software, and the Internet

I. *Hardware:* The industry has been reducing the factor size of microprocessors and peripherals to design actual mobile devices. Before the form factor size was reduced enough, the mobile device could not achieve both small size and processing capability at the same time. We had either a PC-sized laptop computer or a much weaker personal data assistant (PDA) in phone size. Mobile operating systems for PDAs usually did not have full multitasking or 3D graphics support. Features like sensors, such as accelerometers, and capacitor-based touch screens were not available in the past mobile operating systems.

II. *Software:* With a laptop computer, the software is mainly focused on the user's productivity, where support for keyboard and mouse that have precise inputs are essential. The software for a personal data assistant, as its name implies, helps the user to manage personal data such as contacts information, e-mail, and so on. The mobile operating systems were not designed for good responsiveness or smoothness with a rich user interface (UI) including both touch screen and other sensors.

III. *Internet:* Along with Internet development, especially after Web 2.0, there is abundant information in the network waiting to be searched, organized, mined, and brought to users. People are increasingly living with the Internet instead of just browsing the Web. More and more people are involved in the development, including information contribution, application development, and social interactions. The mobile operating systems cannot be self-contained, but have to be open systems.

1. Android OS

The Android platform contains the following layers :

- *Linux Kernel*: Android relies on Linux for core system services such as security, memory management, process management and so on.

- *Android Runtime*: it provides a set of core libraries which supports most of the functionality in the core libraries of Java. The Android Virtual Machine known as Dalvik VM relies on the Linux kernel for some underlying functionality.

- *Libraries*: Android includes a set of C/C++ libraries. These libraries are exposed to developers through the Android application framework. They include media libraries, system C libraries, surface manager, 3D libraries, SQLite and so on.

- *Application Framework*: it provides an access layer to the framework APIs used by the core applications. It allows components to be used by the developers.

2.iOS

iOS (previously iPhone OS) is a mobile operating system developed by Apple Inc. and distributed exclusively for Apple hardware . It is the operating system that powers iPhone, iPad, iPod Touch, and Apple TV. It is closed source and proprietary and built on open source Darwin core OS. iOS promoted a new style of user interaction for small screen, limited input devices, specifically, direct manipulation. Touch-based gestures like swipe, tap, tap and hold, and pinch are used to control on-screen interface elements, and to perform interface operations. Accelerometers support additional physical gestures like shaking and rotating the orientation of the device .iOS is derived from Mac OS X, and shares its basic Darwin foundation, an open source POSIX-compliant UNIX OS. In this sense iOS can be considered a variant of UNIX. iOS is made up of four abstraction layers: Core OS, Core Services, Media, and Cocoa Touch.

- *Core OS:* The kernel of the operating system, which includes basic low-level features: system support—threads, sockets, IO, DNS, math, memory—general security services—certificates, private/public keys, encryption—external hardware management, bluetooth, and sound and image processing.
- *Core Services:* Fundamental system-services, which are subdivided in different frameworks and based on C and Objective C. It includes basic application services, including accounts, contacts, networking, data management, location, calendar events, store purchasing, SQLite, and XML support.

- *Media Layer:* Considers the high-level frameworks, which are responsible for using graphic (support for 2d and 3d graphics), audio-and video technologies.

- *Cocoa Touch:* The UIKIT, which is an Objective- C based framework and provides a number of functionalities, which are necessary for the development of an iOS Application like the User Interface Management. It also includes APIs for building applications—multitasking, touch input, notifications, interface views, and access to device data. Figure 3 below depicts the ioS architecture.

3. Windows Phone

Windows Phone is a successor of the operating system Windows Mobile of the software developer Microsoft. By comparison to the other discussed mobile operating systems, the market share is low with only 4,2%. But like in the previously chapter mentioned can the cooperation between Nokia and Microsoft be rated as a high potential for a market share growth.

Windows Phone uses technologies and tools, which are also, used in the station based application development, like the development environment Visual Studio and the Frameworks Silverlight, XNA and .NET Compact. Furthermore Windows

Phone considers a complete integration with the Microsoft Services Windows Live, Zune, Xbox Live and Bing. For sandboxing Windows Phone uses the same model like Android and iOS . Furthermore 3rd party applications can only be signed with an official certification, like iOS Applications. The following chapter will show the currently available policies of the discussed mobile operating system. Afterwards there will be a summarized comparison of an all mobile operating system policies.

6.2 MOBILE OPERATING SYSTEM POLICIES

A.Android Policies

Since version 2.2 Android offers a Device Administration API, that provides device administration and control features at the system level. With this API, developers can write device management applications that enforce policies. These policies could be hard-coded into the application, or fetched dynamically from a third party server. The API supports following native policies, which are segmented into needed platform version for support.

Android 2.2 or higher:

- Password enabled
- Minimum password length
- Alphanumeric password required
- Maximum failed password attempts
- Maximum inactivity time lock
- Prompt user to set a new password

- Lock device immediately
- Wipe the device’s data (restore the device to its factory defaults)

Android 3.0 or higher:

- Complex password required
- Minimum letters required in password
- Minimum lowercase letters required in password
- Minimum non-letter characters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password
- Password expiration timeout
- Password history restriction
- Maximum failed password attempts

- Maximum inactivity time lock Require storage encryption

B. iOS Policies

- Require passcode
- Allow simple value
- Require alphanumeric value
- Passcode length
- Number of complex characters
- Maximum passcode age
- Time before auto-lock
- Number of unique passcodes before reuse
- Grace period for device lock
- Number of failed attempts before wipe
- Control Configuration Profile removal by user

Restrictions:

- Application installation
- Camera
- Screen capture
- Automatic sync of mail accounts while roaming
- Voice dialing when locked
- In-application purchasing
- Require encrypted backups to iTunes
- Explicit music and podcasts in iTunes
- Safari security preferences
- YouTube
- iTunes Store
- App Store

- Safari

Additionally the Mobile Device Management server can op-erate some actions on the iOS device, like:

- Remote Wipe: A remotely delete of all data on the device, restoring to factory settings

- Remote lock: The Server locks the device and requires the device passcode to unlock it
- Clear passcode: Enables the user to create a new pass-word, if he forgot the old one.

- Configuration and Provisioning Profiles: Give the ability to add and remove configuration profiles remotely

C. Windows Phone Policies

- Password Required

- Minimum Password Length

- Idle Timeout Frequency Value

- Allow Simple Password

- Password Expiration

- Password History

6.3 Comparative Study of Different Mobile Operating Systems

- **Symbian OS**: This operating system which is based on original PDAs from Psion is produced by the software development & licensing company named as “Symbian Ltd”. It was established in June 1998. The native language of the Symbian OS is C++ and therefore this is known as its primary programming language. It has the largest installed base. This operating system is used in Nokia mobiles. From the point of view of software development, it must possess the right SDK and the Integrated Development Environment (IDE) tool of our choice. An IDE generally possess a source editor, compiler and/or interpreter and debugger and is a software application which allows the computer programmer to develop software for a certain platform. The IDE required for Symbian OS is either Carbide C++, Code Warrior or Visual C++. In this the programmer is free to use any programming language.

- **Android OS:** This is a software platform and operating system for mobile devices which is based on Linux kernel and is developed by Google but later on by Open Handset Alliance (OHA) . Its native language is Java which is the officially supported language. In this applications can be written in other languages also but later on it is compiled to ARM native code. This Operating System is used in Samsung, HTC mobiles.

- **IPhone OS (iOS)** : This strong but expensive operating system is developed by Apple whose native language is C. It is also used in iPad, iPhone and iPod touch.

- **BlackBerry OS: This** operating system is developed by Research In Motion for its BlackBerry line of smartphone hand held devices. It provides multitasking & supports specialized input devices that have been adopted by RIM for use in its handhelds especially the trackballs, trackwheel, trackpad and touchscreens. This operating system is designed only in C++ and it supports many languages like US English, UK English, French, etc.

- **Windows Phone 7:** It is also known as Windows Mobile operating system. It is developed by Microsoft that was used in smartphones and mobile devices, but is being currently phased out to specialized markets. The current and last version is "Windows Mobile 6.5". It is based on the Windows CE 5.2 kernel. It is programmed in C++ language.

6.4 TYPES OF MOBILE OS PLATFORMS

The Mobile OSs can be differentiated, based on the existing operating systems used by computers.

a. Real-Time Operating System (RTOS)

Real-Time Operating System which responds to inputs, immediately and generates results, instantly. This type of system is usually used to control scientific devices and similar small instruments where memory and resources are crucial and constricted. This type of devices have very limited or zero-end user utilities, so more effort goes into making the OS really memory efficient and fast (less coding), so as to minimize the execution time ,in turn saving on power as well. e.g.: 8086 etc.

b. Single user, single tasking operation system

This type of OS is better version of Real time OS, where one user can do effectively one thing at a time, which means that doing more than one thing at a time is difficult in this type of OS. For instance: The palm OS in palm hand held computer is an example of single-task OS.

c. Single user, multi-tasking operating system

It allows more than one program to run concurrently like printing, scanning, word processing etc. e.g. MS Windows and Apple’s Mac OS

d. Multi-user operating system

It allows two or more users to run programs at the same time. Some OS permit hundreds or even thousands of concurrent users. e.g. UNIX, and Main Frame OS

6.5 Mobile Operating System (Only features)

Windows CE:-

1. Customize a platform.

2. Component services,

3. Networking capabilities,

4. Multimedia support, and

5. Many other capabilities

- Windows CE is optimized for devices that have minimal memory; a Windows CE kernel may run with one megabyte of memory.
- Devices are often configured without disk storage, and may be configured as a "closed"
  - system that does not allow for end-user extension (for instance, it can be burned into ROM).

- Windows CE conforms to the definition of a real-time operating system, with deterministic interrupt latency.

- From Version 3 and onward, the system supports 256 priority levels and uses priority inheritance for dealing with priority inversion. The fundamental unit of execution is the thread. This helps to simplify the interface and improve execution time.

- A distinctive feature of Windows CE compared to other Microsoft operating systems is that large parts of it are offered in source code form.

- First, source code was offered to several vendors, so they could adjust it to their hardware.
- Then products like Platform Builder (an integrated environment for Windows CE OS image creation and integration, or customized operating system designs based on CE) offered several components in source code form to the general public.
- However, a number of core components that do not need adaptation to specific hardware environments (other than the CPU family) are still distributed in binary only form.

Symbian OS:-

- User interface
- Browser
- Multiple language support
- Application Development

User interface

- Symbian has had a native graphics toolkit since its inception, known as AVKON (formerly known as Series 60).
- S60 was designed to be manipulated by a keyboard-like interface metaphor, such as the ~15-key augmented telephone keypad, or the mini-QWERTY keyboards.
- AVKON-based software is binary-compatible with Symbian versions up to and including Symbian^3. Symbian^3 includes the Qt framework, which is now the recommended user interface toolkit for new applications.

- Qt can also be installed on older Symbian devices. Symbian^4 was planned to introduce a new GUI library framework specifically designed for a touch-based interface, known as "UI Extensions for Mobile"

Browser

- Symbian^3 and earlier have a built-in WebKit based browser. Symbian was the first mobile platform to make use of WebKit (in June 2005).

- Some older Symbian models have Opera Mobile as their default browser.

Multiple language support

- Symbian has strong localization support enabling manufacturers and 3rd party application developers to localize their Symbian based products in order to support global distribution.

- Current Symbian release (Symbian Belle) has support for 48 languages, which Nokia makes available on device in language packs (set of languages which cover the languages commonly spoken in the area where the device variant is intended to be sold).
- All language packs have in common English (or a locally relevant dialect of it).
- Arabic (Arabic),

- Basque (Latin),

- Bulgarian (Cyrillic),

- Catalan (Latin),

- Chinese [PRC] (Simplified Chinese),

- Chinese [Hong Kong] (Traditional Chinese),
- Chinese [Taiwan] (Traditional Chinese),
- Croatian (Latin),
- Czech (Latin),
- Danish (Latin),
- Dutch (Latin),
- English [UK] (Latin),
- etc

Application Development

- From 2010, Symbian switched to using standard C++ with Qt as the main SDK, which can be used with either Qt Creator or Carbide.c++.

- Qt supports the older Symbian/S60 3rd (starting with Feature Pack 1, aka S60 3.1) and Symbian/S60 5th Edition (aka S60 5.01b) releases, as well as the new Symbian platform.

  It also supports Maemo and MeeGo, Windows, Linux and Mac OS X.

6.6Android

- **Android** (from its former owner **Android, Inc.**) is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets.
    - Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input.
    - In addition to touchscreen devices, Google has further developed Android TV for televisions, Android Auto for cars, and Android Wear for wrist watches, each with a specialized user interface.
    - Variants of Android are also used on notebooks, game consoles, digital cameras, and other electronics.

6.6.1Android Overview

1. Android is an open source and Linux-based **Operating System** for mobile devices such as smartphones and tablet computers.

2. Android was developed by the *Open Handset Alliance*, led by Google, and other companies.

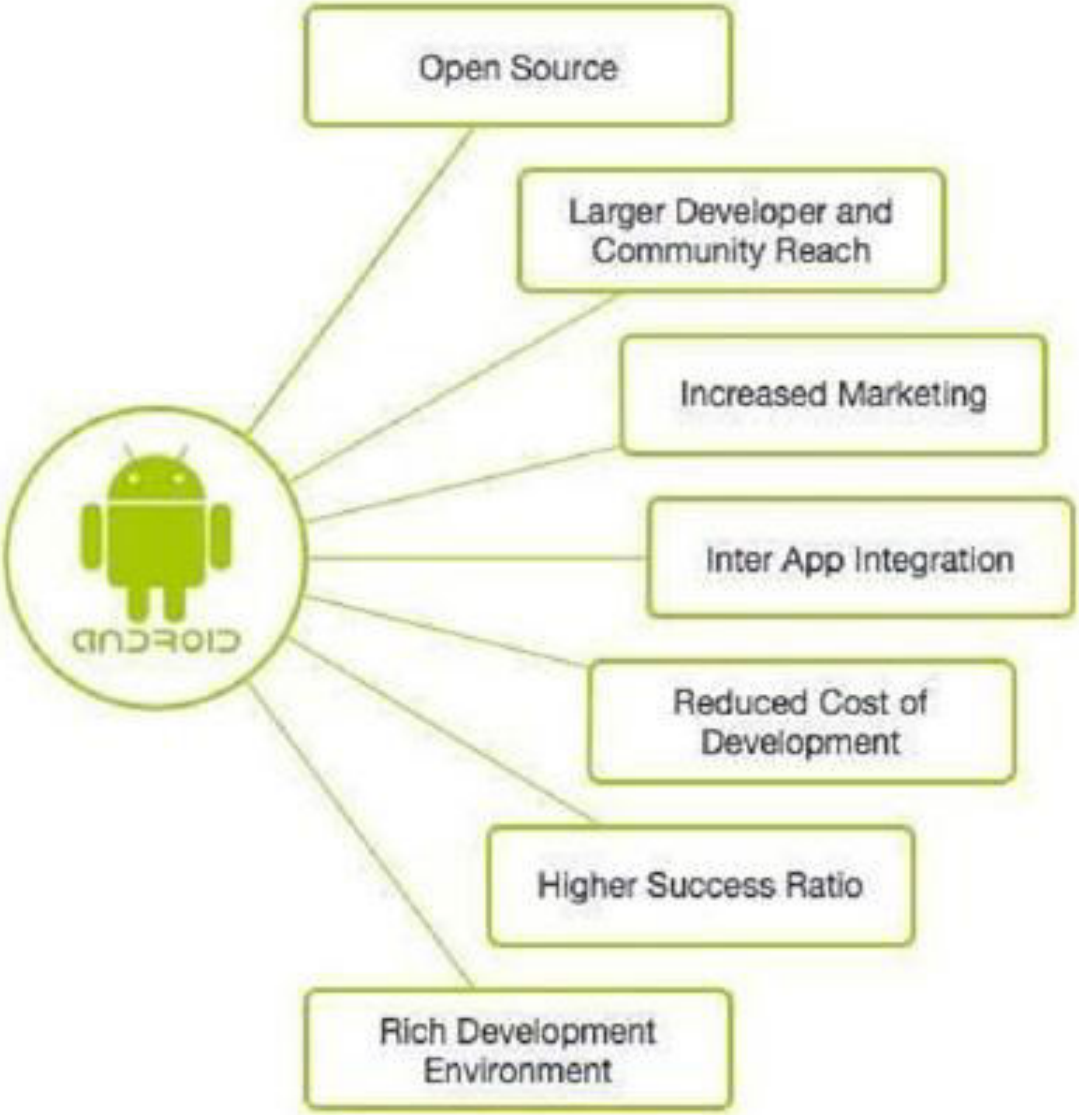
3. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android.

4. The first beta version of the Android Software Development Kit (SDK) was released by Google in 2007 where as the first commercial version, Android 1.0, was released in September 2008.

5. On June 27, 2012, at the Google I/O conference, Google announced the next Android version, 4.1 **Jelly Bean**. Jelly Bean is an incremental update, with the primary aim of improving the user interface, both in terms of functionality and performance.

6. The source code for Android is available under free and open source software licenses. Google publishes most of the code under the Apache License version 2.0 and the rest, Linux kernel changes, under the GNU General Public License version 2.

Why Android?


Open Source
Larger Developer and Community Reach
Increased Marketing
Inter App Integration
Reduced Cost of Development
Higher Success Ratio
Rich Development Environment
android

6.6.2Android Applications

- Android applications are usually developed in the Java language using the Android Software Development Kit.

- Once developed, Android applications can be packaged easily and sold out either through a store such as **Google Play**,**SlideME**,**Opera Mobile Store**,**Mobango**,**F-droid** and the **Amazon Appstore**.

- Android powers hundreds of millions of mobile devices in more than 190 countries around the world.

- It's the largest installed base of any mobile platform and growing fast. Every day more than 1 million new Android devices are activated worldwide.

- This tutorial has been written with an aim to teach you how to develop and package Android application.

- We will start from environment setup for Android application programming and then drill down to look into various aspects of Android applications.

6.6.3Android Architecture

Android architecture or **Android software stack** is categorized into five parts:

- Linux kernel
- native libraries (middleware),
- Android Runtime
- Application Framework
- Applications

.

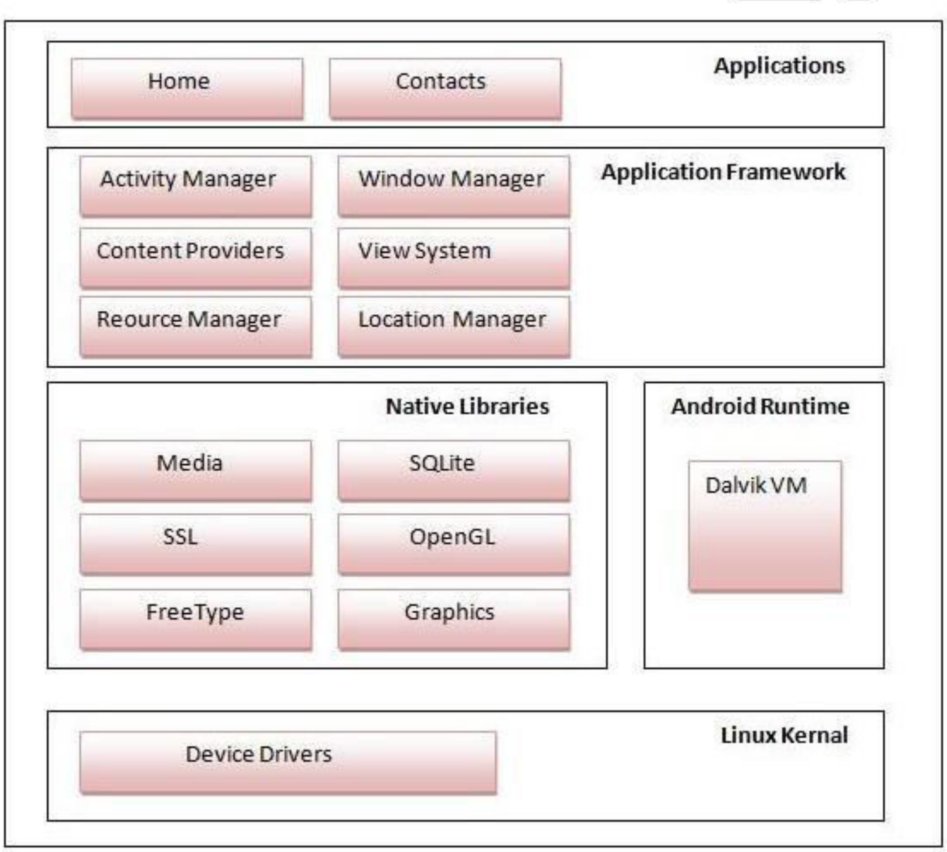


Fig 6.1: Android Architecture

1) Linux kernel

It is the heart of android architecture that exists at the root of android architecture. **Linux kernel** is responsible for device drivers, power management, memory management, device management and resource access.

2) Native Libraries

On the top of linux kernel, there are **Native libraries** such as WebKit, OpenGL, FreeType, SQLite, Media, C runtime library (libc) etc.The WebKit library is responsible for browser support, SQLite is for database, FreeType for font support, Media for playing and recording audio and video formats.

3) Android Runtime

In android runtime, there are core libraries and DVM (Dalvik Virtual Machine) which is responsible to run android application. DVM is like JVM but it is optimized for mobile devices. It consumes less memory and provides fast performance.

4) Android Framework

On the top of Native libraries and android runtime, there is android framework. Android framework includes **Android API's**such as UI (User Interface), telephony, resources, locations, Content Providers (data) and package managers. It provides a lot of classes and interfaces for android application development.

5) Applications

On the top of android framework, there are applications. All applications such as home, contact, settings, games, browsers are using android framework that uses android runtime and libraries. Android runtime and native libraries are using Linux kernel.

6.6.4 Life Cycle of Android Activity

As an activity transitions from state to state, it is notified of the change by calls to the f**ollowing protected methods**:

Void onCreate(Bundle savedInstanceState)

- void onStart()
- void onRestart()
- void onResume()
- void onPause()
- void onStop()
- void onDestroy()

Taken together, these seven methods define the entire lifecycle of an activity

Callback	**Description**
onCreate()	This is the first callback and called when the activity is first created.
onStart()	This callback is called when the activity becomes visible to the user.
onResume()	This is called when the user starts interacting with the application.

onPause()	The paused activity does not receive user input and cannot execute any code and called when the current activity is being paused and the previous activity is being resumed.
onStop()	This callback is called when the activity is no longer visible.
onDestroy()	This callback is called before the activity is destroyed by the system.
onRestart()	This callback is called when the activity restarts after stopping it.

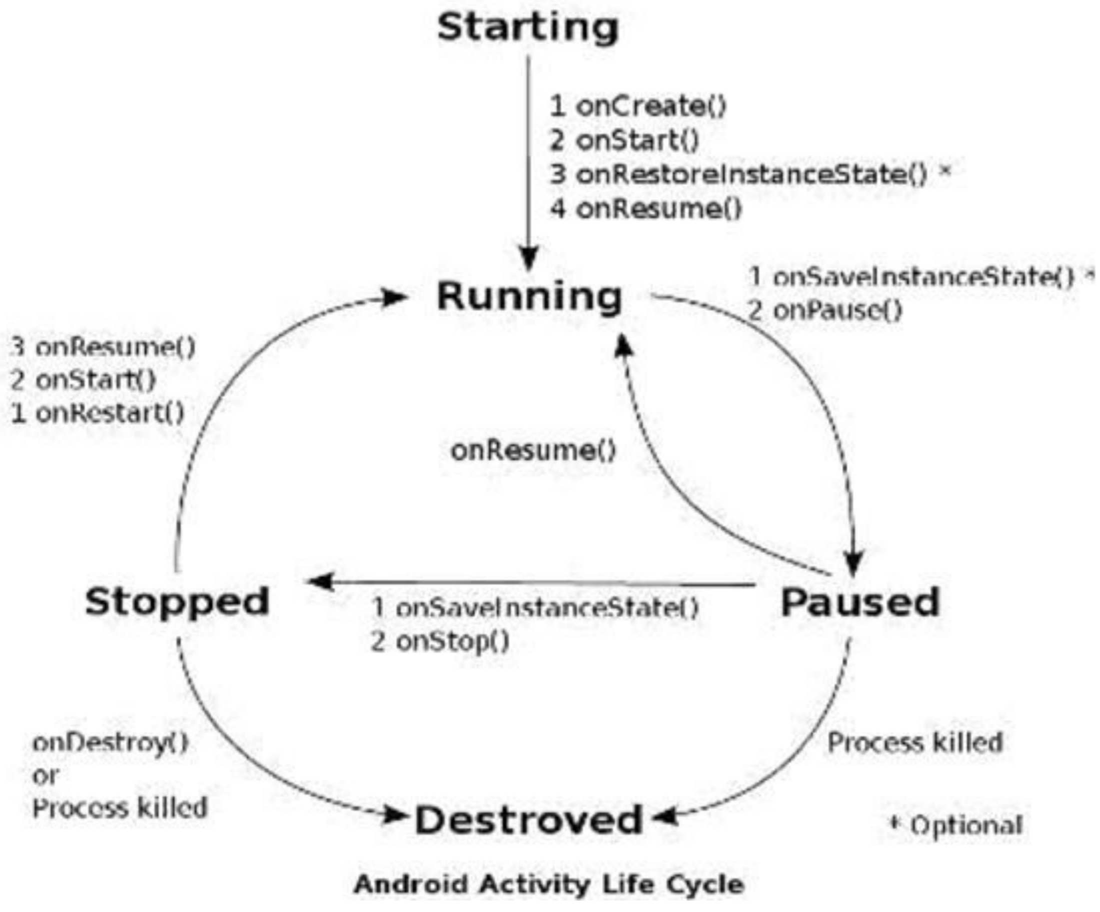


Fig. 6.2: Life Cycle of Android

REFERENCES

[1] B.R. Badrinath, A. Acharya, T. Imielinski, “Impact of Mobility on Distributed Computing”,

[2] *Operating Systems Review*, Vol. 27, No. 2, April 1993.

[3] B.R. Badrinath, G. Welling, “Event Delivery Abstraction for Mobile Computing”, *Technical Report, LCSR-TR-242*, Rutgers University, 1995.

[4] R. Bagrodia. W.W. Chu, L. Kleinrock. G. Popek, “Vision, Issues, and Architecture for Nomadic Computing”, *IEEE Personal Communications*, December 1995.

[5] K. Cheverst, G.S. Blair, N. Davies A. Friday, A.D. Cross, P.F. Raven, “Moving 'Desktop' into the Field”, *IEE Colloquium on Integrating Telecommunications and IT on the Desktop*, London, March 1994.

[6] D.C. Cox, “Wireless Personal Communications: What Is It?”, *IEEE Personal Communications*, April 1995.

[7] N. Davies, G.S. Blair, A. Friday, A.D. Cross, P.F Raven, “Mobile Open Systems Technologies for the Utilities Industries”, *IEE Colloquium on CSCW Issues for Mobile and Remote Workers*, London, March 1993.

[8] N. Davies, S. Pink, G.S. Blair, “Services to Support Distributed Applications in a Mobile Environment”, *Proc. of the 1st International Workshop on Services in Distributed and Networked Environments*, Prague, June 1994.

[9] N. Davies, G.S. Blair, K. Cheverst, A. Friday, “Supporting Adaptive Services in a Heterogeneous Mobile Environment”, *Proc. of IEEE Workshop on Mobile Computing Systems and Applications*, Santa Cruz, California, December, 1994.

[10] A. Demers, K. Peterson, M. Spreitzer, D. Terry, M. Theimer, B. Welch, “The Bayou Architecture : Support for Data Sharing Among Mobile Users”, *Proc. of the IEEE Workshop on Mobile Computing Systems and Applications*, Santa Cruz, California, December, 1994.

[11] F. Douglis, B. Bershad, “Adaptive Disk Spin-down Policies for Mobile Computers”, *Proc. of the* 2^{nd} *USENIX Symposium on Mobile and Location-Independent Computing*, Michigan, USA, April 1995.

[12] D. Durhamp, S.K. Feiner, G.Q. Maguire, “Software Technology for Wireless Mobile Computing”, *IEEE Network Magazine*, November 1991.

[13] D. Duchamp, “Issues in Wireless Mobile Computing”, *Proc. Of the* 3^{rd} *Workshop on Workstation Operating Systems*, IEEE, April 1992.

[14] M.R. Ebling, L.B. Mummert, D.C. Steere, “Overcoming the Network Bottleneck in Mobile Computing”, *Proc. of the IEEE Workshop on Mobile Computing Systems and Applications*, Santa Cruz, California, December, 1994.

[15] A.J. Friday, G.S. Blair, K.W.J Cheverst, N. Davies, “Extensions to ANSAware for Advanced Mobile Applications”, *Proc. of the International Conference on Distributed Platform*, Dresden, Germany, February 1996.

[16] W.C. Grant, “Wireless Coyote : A Computer-Supported Field Trip*”, Communications of the ACM*, Vol. 36, No. 5, May 1993.

[17] B.C. Housel, D.B. Lindquist, “WebExpress: A System for Optimising Web Browsing in a Wireless Environment”, *Proc. of Mobicom '96*, 1996.

[18] T. Imielinski, B.R. Badrinath, “Mobile Wireless Computing : Solutions and Challenges in Data Management”, *Communications of the ACM*, Vol. 37, No. 10, October 1994.

[19] T. Imielinski, M. Gupta, S. Peyyeti, “Energy Efficient Data Filtering and Communication in Mobile Wireless Computing”, *Proc. of the* 2^{nd}